22.2R3-S3: Software Release Notification for JUNOS Software Version 22.2R3-S3

Alert Description

Junos Software Service Release version 22.2R3-S3 is now available for download from the Junos software download site

Download Junos Software Service Release:

1. Go to Junos Platforms - Download Software page
2. Input your product in the "Find a Product" search box
3. From the Type/OS drop-down menu, select *Junos SR*
4. From the Version drop-down menu, select your version
5. Click the Software tab
6. Select the Install Package as need and follow the prompts

NOTE: Starting on August 30th, 2024, we include PR's severity with each entry. See KB86335 for the definition of PR's Severity

Solution

Junos Software service Release version 22.2R3-S3 is now available.

22.2R3-S3 - List of Fixed issues

PR Number	Synopsis	Category: EX4300 PFE
1737587	DDOS log messages will be observed when high traffic is seen Product-Group=junos Severity=Major	The issue is observed on EX4300-24T/EX4300-24P/EX4300-48T/EX4300-48P/EX4300-MP/EX4300-VC/EX4400/EX4100 platforms when high traffic is seen. There will be no service impact.When this issue occurs, the following log messages can be seen-c17-44 jddosd[9001]: DDOS_PROTOCOL_VIOLATION_SET: Warning: Host-bound traffic for protocol/exception Virtual-Chassis:aggregate exceeded its allowed bandwidth at fpc 0 for 184 times, PDTc17-44 jddosd[9001]: DDOS_PROTOCOL_VIOLATION_CLEAR: INFO: Host-bound traffic for protocol/exception Virtual-Chassis:aggregate has returned to normal. Its allowed bandwith was exceeded at fpc 0 for 184 times.
PR Number	**Synopsis**	**Category: EX4300 Platform implementation**
1734925	EX4300-48MP: Device did not come up with USB image when "request system reboot usb" is issued. Product-Group=junosvae Severity=Major	Request system reboot usb doesn't seems to be supported in Ex4300-48MP.
PR Number	**Synopsis**	**Category: EX2300/3400 PFE**
1710360	Certain EX platforms with option-18 configured may hinder the DHCPv6 process Product-Group=junos Severity=Major	DHCPv6 clients drops DHCP Advertise packets as option-18 enabled specific Junos based EX platforms (EX4400, EX2300, EX3400, EX4300-MP, EX4100) which are sitting between the relay and the client, are sending malformed packets.
1721433	On EX2300MP, error messages are observed during reboot/image upgrade Product-Group=junos Severity=Major	Logs dc-pfe[16077]: PFE_BRCM_COS_HALP_ERR: BRCM_COS_HALP(brcm_block_cpu_traffic:2383):Port MMU Traffic setting skipped (Feature unavailable) Feature port MMU traffic setting is not supported on EX2300 platform due to which logs were displayed. These logs are not functionality impacting.
1766314	Memory leak is observed when dot1x authentication is used Product-Group=junos Severity=Major	On EX and QFX5K series platforms, in scenarios where CWA (Central Web Authentication) or Captive Portal are used as the second level of authentication after MAC is authenticated as part of dot1x, memory is leaked in PFE for every http request received at the switch before second level of authentication. When the heap memory utilization crosses 80 percent, a crash is observed and the PFE is restarted with the subsequent impact on the traffic.

PR Number	Synopsis	Category: EX2300/3400 platform
PR Number	**Synopsis**	**Category: MX/PTX 20A AC power Software Issues**
1745299	Fans may stop working after removal and insertion of Fan Tray Product-Group=junosvae Severity=Major	On MX10004/MX10008/MX10016 and Junos-based PTX10004/PTX10008/PTX10016 platforms, some Enhanced fans could not be working after hot-insertion of Fan Tray
PR Number	**Synopsis**	**Category: QFX Control Plane Analyzer related**
1705015	Port-mirroring state remains down on Junos QFX5K platforms Product-Group=junos Severity=Major	For the QFX5K series, while applying the ERSPAN configuration along with the ERSPAN output/egress INET interface configuration sometimes leads to the analyzer not getting created in the HW.
PR Number	**Synopsis**	**Category: QFX VC Datapath**
1779112	After rebooting the VC device with 100G VCP port traffic drop observed on ipv4 and ipv6 streams Product-Group=junos Severity=Critical	When VC is formed with qfx5110-32q and qfx5110-48s, 0.2% traffic drop issue with 40G/100G optics will be seen only with line rate traffic upon reboot
PR Number	**Synopsis**	**Category: SPC3 HW and SW Issues**
1749584	SRX device will take time to come up in HA or device will go down in standalone setup Product-Group=junos Severity=Major	For SRX Platforms with SPC3 cards in cluster configuration, One of the node in cluster will go down as FPC(Flexible PIC Concentrators) takes extra time to reset. In standalone setup, device will go down.
1753108	The spcd process crash will be observed which will restart the SPC3 cards Product-Group=junos Severity=Major	On Junos SRX5K platforms with SPC3 cards, spcd process crash will be observed due to a context switching of an internal thread. The spcd process crash will restart the SPC3 cards which would impact the traffic through the affected card.
1774707	SPC3 PIC heartbeat failure Product-Group=junos Severity=Major	SRX high end chassis SPC3 card PIC can encounter an unexpecting condition not responding to heartbeats, leading to the SPC card reboot.
PR Number	**Synopsis**	**Category: SRX DNS DGA and tunneling related**
1727122	Nstraced process is running high on the primary node after the Junos upgrade Product-Group=junos Severity=Major	On all Junos SRX/vSRX platforms, nstraced process spikes to 100% usage after upgrading to Junos version 21.4R3-S2 or any later releases without having any traces/debugs explicitly configured in the RE (Routing Engine) or PFE (Packet forwarding Engine) of the device.
1755484	Junos OS: SRX Series: If DNS traceoptions are configured in a DGA or tunnel detection scenario specific DNS traffic leads to a PFE crash (CVE-2024-39529) Product-Group=junos Severity=Major	A Use of Externally-Controlled Format String vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS on SRX Series allows an unauthenticated, network-based attacker to cause a Denial-of-Service (DoS). Please refer to https://supportportal.juniper.net/JSA82988 for more information.
PR Number	**Synopsis**	**Category: 5G CUPS - RMPS subsystem**
1662691	some packages name missing which is RMPSD and MOBILED in show version detail command output Product-Group=junos Severity=Major	The version details for certain daemons will appear in the command output after the device has been rebooted after the completion of the USB installation of Junos.
PR Number	**Synopsis**	**Category: Accounting Profile**

1692411	Error messages are observed and incorrect values are returned for SNMP requests for pfe traffic statistics Product-Group=junos Severity=Major	pfed: PFED_NOTIF_GLOBAL_STAT_UNKNOWN: xxxx in syslog The above log messages will be seen when we are using SNMP and if its trying to poll "show pfe statistics notification" through MIB OID - 1.3.6.1.4.1.2636.3.44.1.1.2.1.2.
PR Number	**Synopsis**	**Category: OAM support on ACX**
1746304	Node-segment reachability will be lost in Multitopology based IS-IS Product-Group=junos Severity=Major	On all Junos and Junos OS Evolved platforms, in a Segment Routing MPLS(Multi Protocol Label Switching) environment using IS-IS and an alternate IPv6 unicast topology is configured in addition to the normal IPv4 unicast topology, the node-segment reachability might be lost resulting in traffic loss. This will only happen when the 'family inet6' is configured on the interface without configuring the IPv6 address.
PR Number	**Synopsis**	**Category: ACX GE, 10GE, PoE, IDT framers**
1735670	The command "show interfaces diagnostics optics" shows Tx laser as enabled even when the port is administratively down Product-Group=junos Severity=Major	On ACX5448 platforms, the Tx laser is not turned off even if the port is disabled. This can be identified with the command show interfaces diagnostics optics. There is no service impact due to this issue.
PR Number	**Synopsis**	**Category: "agentd" software daemon**
1715377	The agentd would become unresponsive on all Junos platforms Product-Group=junos Severity=Major	When using Junos Telemetry Interface (JTI) with subscriptions to Packet Forwarding Engine (PFE) based sensors, agentd might slowly leak memory. After prolonged runtime agentd may stop functioning properly, which will affect JTI data export. This will affect telemetry services.
1732763	The xmlproxyd crash might be observed when there are multiple collectors Product-Group=junos Severity=Major	The Xmlproxyd crash could be seen if there are multiple collectors subscribing for Xmlproxyd sensors and some or all of the collectors are flapping frequently at the rate of 90 seconds or so.The occurrence of this issue is rare.The telemetry streaming of Xmlproxyd sensors will be absent during the time Xmlproxyd crashes and restarts on its own. This time could be within 30 seconds or so.Once Xmlproxyd comes up, the telemetry streaming of Xmlproxyd sensors will be resumed automatically.
1752412	gRPC telemetry intermittently miss reporting is_wrap flag Product-Group=junos Severity=Critical	On all Junos platforms when telemetry is enabled, gRPC telemetry message contain a metadata flag is_wrap that indicate to the telemetry client that all telemetry data for the specific Xpath is reported for the specific round. This flag may not be reported intermittently in some edge cases.
PR Number	**Synopsis**	**Category: MPC10/11/LC9600 Chassis Category**
1742510	Tunnel interfaces are getting bounced causing a momentary impact on traffic Product-Group=junos Severity=Major	On MX304 device and LC9600 line card, upon Routing Engine switchover chassisd on new master was not re-initializing the tunnel/inline services configuration data, hence all static tunnel interface (GRE, IP-IP, Multicast (MT), PIM, Logical tunnels and Virtual loopback tunneling (VT)) and inline interfaces will get bounced (deleted and re-created) after doing any CLI commit after an RE switchover. There will be momentary impact on traffic using these interfaces.
PR Number	**Synopsis**	**Category: MX YT-ZF Linecards Fabric Software Category**
1689523	Ungraceful FPC reboot causes drain timeouts in adjacent FPCs and fails to restore traffic Product-Group=junos Severity=Major	On MX10004 and MX10008 platforms with LC9600, if a Flexible PIC Concentrator (FPC)(LC9600) reboots ungracefully, it results in peer LC9600 FPCs (residing on the same chassis) sending heavy fabric traffic to the failing FPC to have fabric streams stuck in drain timeout. Both ungraceful FPC reboot and heavy fabric traffic to the failing FPC lead to the issue.
PR Number	**Synopsis**	**Category: MPC Fusion SW**
1744883	100G interfaces will flap due to RE switchover on Junos	On Junos MX platforms with MPC3E-3D-NG/MPC-3E-3D-NG-Q linecards, 100G

	MX platforms with MPC3E-3D-NG/MPC-3E-3D-NG-Q linecards Product-Group=junos Severity=Major	interfaces will flap due to RE (Routing Engine) switchover.
PR Number	**Synopsis**	**Category: Application Quality of Experience**
1790782	The srxpfe or flowd process will crash while trying to update the path probe statistics Product-Group=junos Severity=Major	On Junos SRX300, SRX320, SRX340, SRX345, SRX380, SRX1500, SRX4100, SRX4200, SRX4600, vSRX2, vSRX3, and NFX platforms, while trying to update the path probe statistics the flowd/srxpfe process will crash when APPQOE best path changes to no path selected state. The process crash will restart the PFE affecting the traffic.
PR Number	**Synopsis**	**Category: SRX2000/50000 issue**
1784775	The chassis cluster failover is seen post ISSU Product-Group=junos Severity=Major	On SRX5K platforms with SPC3, chassis cluster failover is seen post ISSU. The SPC3 connects to the wrong Routing Engine which impacts all the PICs affecting the complete traffic.
1787219	Insufficient power alarm observed in SRX5K platforms Product-Group=junos Severity=Major	On Junos SRX5600 and SRX5800 platforms, FPC (Flexible PIC Concentrator) will not come online due to insufficient power, leading to service disruption.
PR Number	**Synopsis**	**Category: PFE issue for flowd on australia SPU**
1726888	SNMP MIB walk for ipSystemStatsTable takes a long time to dump the output Product-Group=junos Severity=Major	When polling ip SystemStatsTable, the responses have noticable delay
1727027	The datapath-debug packet-dump feature is not capturing the transit traffic packets Product-Group=junos Severity=Major	On SRX5000 platforms with IOC3 card (SRX5K-MPC3-100G10G and SRX5K-MPC3-40G10G), datapath-debug packet-dump will stop capturing the transit traffic packets when datapath-debug packet filters with packet-dump are targeting the traffic on the interface which is configured with firewall filters.
PR Number	**Synopsis**	**Category: common or misc area for SRX product**
1715048	Junos devices not return any values when polling SNMP MIB jnxPsuChassisPowerConsumed Product-Group=junos Severity=Major	Junos devices not return any values when polling SNMP MIB jnxPsuChassisPowerConsumed. Multiple platforms (including MX, EX, QFX, ACX and SRX5K) are affected by this issue.
PR Number	**Synopsis**	**Category: BBE Advanced Services related issues**
1735560	The bbe-smgd crash can be seen in a certain scenario Product-Group=junos Severity=Major	On Junos MX platforms supporting subscriber services, the bbe (broadband edge)-smgd (subscriber management daemon) crash can be observed due to memory consumption which will impact subscribers from bringing up.
PR Number	**Synopsis**	**Category: BBE interface related issues**
1734564	Junos OS: MX Series: Memory leak in bbe-smgd process if BFD liveness detection for DHCP subscribers is enabled (CVE-2024-21587) Product-Group=junos Severity=Major	An Improper Handling of Exceptional Conditions vulnerability in the broadband edge subscriber management daemon (bbe-smgd) of Juniper Networks Junos OS on MX Series allows an attacker directly connected to the vulnerable system who repeatedly flaps DHCP subscriber sessions to cause a slow memory leak, ultimately leading to a Denial of Service (DoS). Please refer to https://supportportal.juniper.net/JSA75725 for more information.
PR Number	**Synopsis**	**Category: BBE network stack related issues**
1751656	ARP learning issue for dynamic ARP entry for the DVLAN stacked frame route not resolved	On MX platforms with Subscriber Management and knob "ipoe-dynamic-arp-enable" configured, the L2 (MAC address) in the frame route will be incorrect

	Product-Group=junos Severity=Major	due to which traffic flow for VLAN subscribers will get impacted as dynamic ARP entry for the DVLAN (Dynamic VLAN) stacked frame route won't get resolved resulting in ARP learning issue.
PR Number	**Synopsis**	**Category: Bi Directional Forwarding Detection (BFD)**
1675921	Micro BFD session state in RE remain UP even peer side session is down. Product-Group=junos Severity=Major	Any platforms with Micro BFD configured on member links of the LAG/ae interface, BFD Session state in RE remains as UP always even though PEER device has ceased.
1698373	A few BFD sessions might flap after FPC reload and stabilization Product-Group=junos Severity=Major	On all Junos platforms and Junos Evolved with scaled BFD sessions, FPC reload/restart results in few BFD session flap.
1706018	The BFD session would flap when the GRES is triggered with single-hop BFD over AE interfaces configured Product-Group=junos Severity=Major	On all Junos and Junos Evolved platforms, Bidirectional Forwarding Detection (BFD) sessions would flap and leads to route churn in the network when the Graceful Routing Engine Switchover (GRES) is triggered with single-hop BFD sessions over Aggregated Ethernet (AE) interfaces. It is a timing issue.
PR Number	**Synopsis**	**Category: Border Gateway Protocol**
1448092	unexpected delay while running "show route advertising-protocol bgp" for an unconfigured peer in scaled vrf Product-Group=junos Severity=Minor	When we have a large route volume to iterate/display, the show route advertising-protocol bgp takes more time to return for an unconfigured peer.
1687887	More than expected traffic loss is seen with ECMP FRR enabled during link down scenario Product-Group=junos Severity=Major	On all Junos and Junos Evolved platforms, in a link down/BFD down event, traffic loss is seen to occur more than expected with ECMP fast reroute (FRR) or BGP Prefix-Independent Convergence (PIC) configured.
1689904	BGP LU Advertisements fail with the message "BGP label allocation failure: Need a gateway" Product-Group=junos Severity=Major	On all Junos and Junos Evolved platforms BGP-LU (Border Gateway Protocol Labeled-Unicast) Advertisements fail with the message "BGP label allocation failure: Need a gateway" based on timing conditions involving route resolution and installation.
1692320	Deletion and addition of BGP transport-class caused the rpd crash Product-Group=junos Severity=Critical	On all Junos and Junos Evolved platforms deletion and addition of transport-class on top of BGP CT configuration and NSR configuration the rpd crash seen. commit synchronization process during config commit doesn't work for auto-created routing instances, created by BGP-CT transport classes.
1695050	The rpd process crash is seen when logical systems shutdown does not complete Product-Group=junos Severity=Major	On all Junos and Junos Evolved platforms, when logical systems is configured with 'family route-target', there is a certain corner case scenario where logical systems shutdown does not complete on a 'deactivate logical-system' causing rpd process crash.
1696870	BGP scheduler slips during sub-optimal prefix-walk while deleting selected prefixes from a large set. Product-Group=junos Severity=Minor	On all Junos and Junos Evolved platforms, you might see the BGP scheduler slip while deleting a large set of prefixes.
1709837	Junos OS and Junos OS Evolved: A crafted BGP UPDATE message allows a remote attacker to de-peer (reset) BGP sessions (CVE-2023-4481) Product-Group=junos Severity=Critical	An Improper Input Validation vulnerability in the Routing Protocol Daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS). Please refer to https://supportportal.juniper.net/JSA72510 for more information.
1712527	The PE advertises incorrect next-hop towards CE although BGP export policy configured with next-hop under policy-statement Product-Group=junos Severity=Major	The show route advertising-protocol bgp reporting nexthop self rather than IP in the configured policy-statement for next-hop.
1716946	BGP connection doesn't establish when it is configured with rfc8950-compliant under logical-systems on all	BGP (Border Gateway Protocol) session/connection is not getting up and keeps flapping when rfc8950-compliant and extended-nexthop are configured with BGP

	Junos and Junos OS Evolved platforms Product-Group=junos Severity=Major	under logical-systems on all Junos and Junos OS Evolved platforms.
1728455	The rpd process crashes when BGP is cleaned up Product-Group=junos Severity=Major	On Junos and Junos OS Evolved platforms, if static default RT-C (Route Target - Constrain) is configured when Border Gateway Protocol (BGP) is cleaned up (whole BGP is cleaned up), the routing process will crash.
1729733	BMP leads to prolonged high rpd CPU utilization upon committing the BGP peer import policy configuration Product-Group=junos Severity=Major	On all Junos and Junos Evolved platforms, with BGP Monitoring Protocol (BMP) configured when a Border Gateway Protocol (BGP) peer import policy configuration change is committed that triggers the BGP reconfiguration job for routes re-evaluation, then high Routing Protocol Daemon (rpd) CPU utilization up to 100% will be observed for a long time which may impact routing as high rpd utilization can starve some processes.
1731803	Junos OS and Junos OS Evolved: The rpd will crash upon receiving a malformed BGP UPDATE message (CVE-2023-44204) Product-Group=junos Severity=Major	An Improper Check or Handling of Exceptional Conditions vulnerability in Routing Protocol Daemon (rpd) Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS). Please refer to https://supportportal.juniper.net/JSA73170 for more information.
1732087	The rpd process will crash in a scaled BGP setup with traceoptions configured Product-Group=junos Severity=Major	On all Junos and Junos Evolved platforms in a scaled Border Gateway Protocol (BGP) setup with different Hold timers and BGP trace options enabled, the rpd process will crash when multiple BGP sessions are enabled/disabled.
1737679	The rpd crash files are seen due to a use-after free of objects Product-Group=junos Severity=Major	On all Junos and Junos Evolved platforms, due to a use-after free of objects that are being shared across threads for tracing that happened when some assumptions were broken in a recent fix. The crash files generated in rare conditions when the object is freed prior to when the trace is cut.
1742287	Junos OS and Junos OS Evolved: BGP session flaps on NSR-enabled devices can cause rpd crash (CVE-2024-21585) Product-Group=junos Severity=Major	An Improper Handling of Exceptional Conditions vulnerability in BGP session processing of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated network-based attacker, using specific timing outside the attacker's control, to flap BGP sessions and cause the routing protocol daemon (rpd) process to crash and restart, leading to a Denial of Service (DoS) condition. Please refer to https://supportportal.juniper.net/JSA75723 for more information.
1742416	RPD scheduler slip is observed when the BGP session flaps and subsequent configuration changes for the same peer Product-Group=junos Severity=Major	On all Junos and Junos Evolved platforms, high CPU (RPD scheduler slips) leads to session timeouts/flaps for other protocols running in the system.
1742513	Configuring BGP in routing-instance of type virtual-router resulting in PFE utilizing more memory resources Product-Group=junos Severity=Major	On all Junos and Junos OS Evolved platforms, when Border Gateway Protocol (BGP) is configured in a routing instance virtual router without Layer 3 Virtual Private Network (L3VPN) configuration, the default Multiprotocol label switching (MPLS) table is created unexpectedly for the virtual router instance routing table. There is no functional impact due to this issue apart from extra memory resources being consumed by the Packet Forwarding Engine (PFE).
1744801	Junos OS and Junos OS Evolved: BGP multipath incremental calculation is resulting in an rpd crash (CVE-2024-39554) Product-Group=junos Severity=Critical	A Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') vulnerability the Routing Protocol Daemon (rpd) of Juniper Networks Junos OS and Juniper Networks Junos OS Evolved allows an unauthenticated, network-based attacker to inject incremental routing updates when BGP multipath is enabled, causing rpd to crash and restart, resulting in a Denial of Service (DoS). Since this is a timing issue (race condition), the successful exploitation of this vulnerability is outside the attacker's control. However, continued receipt and processing of this packet may create a sustained Denial of Service (DoS) condition. Please refer to https://supportportal.juniper.net/JSA83014 for more information.
1750441	Junos OS and Junos OS Evolved: A malformed BGP tunnel encapsulation attribute will lead to an rpd crash (CVE-2024-30395) Product-Group=junos Severity=Major	An Improper Check for Unusual or Exceptional Conditions vulnerability in Routing Protocol Daemon (RPD) of Junos OS and Junos OS Evolved allows an unauthenticated, network-based attacker to cause Denial of Service (DoS). Please refer to https://supportportal.juniper.net/JSA79095 for more information.

1754935	BGP multipath route is not correctly applied after changing the IGP metric Product-Group=junos Severity=Major	On all Junos and Junos Evolved platforms, multipath route is not correctly applied due to this Equal-cost multi-path (ECMP) will not be formed, when Border Gateway Protocol (BGP) multipath is configured and the Interior Gateway Protocol (IGP) metric of a network is modified and subsequently reverted.
1755287	Junos OS and Junos OS Evolved: Malformed BGP UPDATE causes rpd crash (CVE-2024-39552) Product-Group=junos Severity=Major	An Improper Handling of Exceptional Conditions vulnerability in the routing protocol daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows a network based, unauthenticated attacker to cause the rpd process to crash leading to a Denial of Service (DoS). Please refer to https://supportportal.juniper.net/JSA75726 for more information.
1758179	The rpd process will crash when L3VPN and eBGP advertise the same route Product-Group=junos Severity=Major	On all Junos and Junos Evolved, in an interception of per-prefix-label and Carrier supporting Carrier (CsC) scenario, if prefix is received both from eBGP-LU and iBGP, the rdp process will crash breaking routing application services.
1760356	Junos OS and Junos OS Evolved: A malformed BGP tunnel encapsulation attribute will lead to an rpd crash (CVE-2024-21598) Product-Group=junos Severity=Major	An Improper Validation of Syntactic Correctness of Input vulnerability in the Routing Protocol Daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows a network-based, unauthenticated attacker to cause a Denial of Service (DoS). Please refer to https://supportportal.juniper.net/JSA75739 for more information.
1760885	The BGP LU labels can have next-hops pointing to each other in multi-homed PE setup Product-Group=junos Severity=Major	On all Junos and Junos Evolved platforms the routes received by two multi-homed PE (Provider Edge) routers in the 'inet-unicast' family are advertised in the BGP (Border Gateway Protocol) LU (Labeled Unicast) family to each other. This issue happens when there is no rib.inet3 configured under the address family labeled unicast which causes the routes from 'inet-unicast' and 'inet-labeled-unicast ' tables to get mixed. There will be a traffic impact when this issue is encountered.
1775548	The rpd crash can be seen with a scaled BGP sharding setup Product-Group=junos Severity=Major	On all Junos and Junos OS Evolved platforms the rpd (Routing Protocol Daemon) crash can be seen in scaled setup. The issue will be seen in the BGP (Border Gateway Protocol) RIB (Routing Information Base) sharding scenario. This issue is very unlikely to be encountered.
1779533	The RPD crash is observed on Junos and Junos Evolved platforms in Route Reflector scenario Product-Group=junos Severity=Major	On all Junos and Junos Evolved platforms, the RPD (Routing Protocol Daemon) crash can be seen in BGP-multipath scenario if it has more than 512 routes for a prefix. The RPD crash will cause a traffic drop but the system will self-recover.
PR Number	**Synopsis**	**Category: Track PRs in BGP programmability area using JET APIs.**
1699356	The rpd core will be seen when the route monitor stream times out Product-Group=junos Severity=Critical	On all Junos and Junos Evolved platforms supporting prpd (programmable routing protocol process), when the route monitor stream times out because of any reason, rpd (routing protocol daemon) core will be seen.
PR Number	**Synopsis**	**Category: Track PRs in BGP BMP area & is part of BGP inside RPD.**
1741732	The BGP routes gets stuck in BMP withdraw state Product-Group=junos Severity=Major	On all Junos and Junos Evolved platforms, in some scenario BMP advertises damped routes as withdraw route in post-policy even if those damped routes become usable and in active state.
PR Number	**Synopsis**	**Category: BGP Openconfig and Sensor**
1714087	Traffic loss is seen on telemetry streaming in BGP sharding environment Product-Group=junos Severity=Major	On all Junos and Junos Evolved platforms RPD core is seen on telemetry streaming with BGP sharding enabled.
PR Number	**Synopsis**	**Category: Issues related to Common BIOS on x86 based designs**
1608045	LTS19: MX960: 000: [Firmware Bug]: TSC_DEADLINE disabled due to Errata; please update microcode to	

	version: 0x3a (or later) seen upon upgrade to 21.4 Product-Group=junos Severity=Major	
PR Number	**Synopsis**	**Category: BBE Remote Access Server**
1740912	Subscribers sessions are logged out after performing GRES Product-Group=junos Severity=Major	On MX platforms with subscriber management scenario, subscribers sessions are logged out in the backup Routing Engine (RE) after performing Graceful Routing Engine Switchover (GRES) .
1759048	Test aaa command may failure due to "Subscriber creation failed" Product-Group=junos Severity=Major	Start from Junos 22.2R1 with flex license enabled releases, test aaa command may failure due to "Subscriber creation failed".
PR Number	**Synopsis**	**Category: Express Broadway PFE L3**
1725716	The error logs "fpc0 expr_hostbound_packet_handler: Receive pe 254?" would be generated Product-Group=junos Severity=Major	On QFX10002-60C and PTX10k platforms, an error log can be generated repeatedly with the base configuration.
PR Number	**Synopsis**	**Category: MX304 Chassis specific platform**
1731237	MX304 Major Alarm " Host 0 detected AER correctable error" after RE switchover. Product-Group=junos Severity=Major	MX304 Major Alarm " Host 0 detected AER correctable error" after RE switchover.
1755788	LT sub-interfaces which are not on the same PIC as the RLT interface goes down after activating RLT interface Product-Group=junos Severity=Major	On MX304 platforms and MX platforms with LC9600 cards supporting RLT (Redundant Logical Tunnel) interfaces, when a RLT interface is activated which has member interfaces across PICs, the LT (Logical Tunnel) sub-interfaces which are not part of the RLT and not on the same PIC (Physical Interface Card) as the RLT interface, goes down. The LT sub-interfaces come up once the RLT interface is deactivated. Since the LT sub-interfaces are not part of the RLT, there is no impact for the same RLT.
PR Number	**Synopsis**	**Category: MX304 line card platform software**
1739718	Incomplete FPC Firmware details will be displayed Product-Group=junos Severity=Major	On MX304 and MX platforms with MPC11 and LC9600, the CLI command 'show system firmware' may sometimes not display all the firmware details of FPC components. This prevents the FPC firmware components from being upgraded to the latest version when the firmware upgrade is performed.
PR Number	**Synopsis**	**Category: MX Platform SW - FRU Management**
1739922	FPC crashes and remains offline after the upgrade of RE BIOS to 0.15.1 version Product-Group=junos Severity=Major	On MX204 and EX9251 platforms running Junos 21.4 or later, the Flexible PIC Concentrator (FPC) crashes and will remain offline after upgrading the RE (Routing Engine) BIOS to 0.15.1 version without power cycling the chassis. This will result in total traffic loss.
PR Number	**Synopsis**	**Category: Virtual-chassis platform/chassisd infrastructure PRs for MX**
1774302	MXVC:MPC10E can not reach VC-Mm when re1 is VC-Mm Product-Group=junos Severity=Major	MXVC:MPC10E can not reach VC-Mm when re1 is VC-Mm. The issue happens only for Linux Based cards and Ukern ie non Linux based cards will work fine.
PR Number	**Synopsis**	**Category: MX2010 platform software**
1774558	"FI: Cell underflow at the state stage" and "FI: Reorder	On all MX platforms with MPC9E line card and Packet forwarding Engine (PFE)

	cell timeout" error is seen impacting forwarding traffic on all MX platforms Product-Group=junos Severity=Major	Application-Specific Integrated Circuits (ASIC) based fabric, if image upgrade is performed then FPC reports "Cell underflow at the state stage" and "reorder cell timeout" messages and live forwarding traffic will be dropped as due to some internal scenarios 200G idles are getting programmed instead of 400G on Switch Processor Mezzanine Board (SPMB).
PR Number	**Synopsis**	**Category: Class of Service**
1719028	The cosd process crash might be seen on all Junos platforms Product-Group=junos Severity=Major	On all Junos platforms when the number of supported queues exceeds above 12, the cosd (Class of Service Daemon) process crash will be seen in an extremely rare scenario.
1757003	Junos OS: MX Series: In a scaled subscriber scenario if CoS information is gathered, the mgd processes get stuck (CVE-2024-21610) Product-Group=junos Severity=Major	An Improper Handling of Exceptional Conditions vulnerability in the Class of Service daemon (cosd) of Juniper Networks Junos OS on MX Series allows an authenticated, network-based attacker with low privileges to cause a limited Denial of Service (DoS). Please refer to https://supportportal.juniper.net/JSA75751 for more information.
1760817	Change in the cosd behaviour due to the CoS interface specific wildcards Product-Group=junos Severity=Major	On all Junos platforms, applying the class-of-service (CoS) interface specific wildcards was leading to an inconsistent behaviour of the class-of-service daemon (cosd) at different times.
PR Number	**Synopsis**	**Category: Enhanced Broadband Edge support for cos**
1769800	The traffic shaping rate gets impacted in a subscriber scenario on Junos MX BBE platforms Product-Group=junos Severity=Major	The traffic shaping rate gets impacted on Junos MX BBE (Broadband Edge) platforms configured with COS (Class Of Service) and when TLV (Type, Length, and Value)#98 is configured on the external OLT (Optical Line Terminal) (which is most likely a default on the OLT in case PON (Passive Optical Network) TLV are activated) for PPPoE-IA (Point-to-Point Protocol over Ethernet) IFLset (interface-set) of the IFD (Interface Device) which allows a single subscriber to limit the throughput of the entire interface.
PR Number	**Synopsis**	**Category: QFX Access Control related**
1778056	Core dumps for pfex and dot1x seen due to dot1x authentication Product-Group=junos Severity=Major	On all Junos platforms, core dumps for Pfex and dot1x will be seen, when dot1x is authenticated. It is a scenario of basic authentication where EAP (Extensible Authentication Protocol) packets are being received from the client.
PR Number	**Synopsis**	**Category: QFX Control Plane VXLAN**
1749759	Traffic discarded on QFX5K platforms in multi-homed EVPN-VXLAN scenario Product-Group=junos Severity=Major	It is observed that on Junos QFX5K platforms when multi-homed EVPN-VXLAN is configured, traffic gets discarded as ARP and NDP next-hop fails to be programmed in PFE because underlying next-hop is missing which is the shared vxlan load-balancing next-hop.
1758783	Traffic is black-holed on QFX5K platforms in EVPN-VXLAN scenario Product-Group=junos Severity=Major	On Junos and Junos Evolved QFX5K platforms, under certain circumstances, the l2ald does not update Virtual Tunnel Endpoint (VTEP) ifl tokens in the kernel which passes them on to Packet forwarding engine (PFE). These tokens are used to create Virtual Port Link Aggregation (VPLAG) next hops in these platforms. Without them, Media Access Control (MAC) routes are incomplete or not created, leading to traffic drop.
PR Number	**Synopsis**	**Category: Platform PR for 1G/10G LC**
1739595	The FPC will core and crash in a race condition Product-Group=junos Severity=Major	On all Junos and Junos Evolved platforms, in a rare scenario, the FPC will go down due to core.
1756780	HMC errors will be observed on Junos platforms with LC480 Product-Group=junosvae	On Junos platforms with LC480 line card when there is high volume of traffic on the line card, HMC (Hybrid Memory Cube) errors are seen due to non-optimal settings on the power regulator device. PFE (Packet forwarding Engine) will be

	Severity=Major	disabled due to these errors and traffic for all ports mapped to that PFE will be impacted.
PR Number	**Synopsis**	**Category: 1G/10G LC Timing software**
1583496	Error message seen in clksyncd logs with SyncE/PTP configs "ESYNC-Error:ferrari_zl30362_reg_write: Error, EEC(0) not yet initialized" Product-Group=junos Severity=Major	Error message seen on MX10K8 chassis with SyncE/PTP configurations, This does not affect any functionality, The error seen here because the API called is specific to ferrari platform which needs to be vecterized.
PR Number	**Synopsis**	**Category: Device Configuration Daemon**
1742124	DCD crash can be seen sometimes while pushing config using API Product-Group=junos Severity=Critical	On all Junos platforms, dcd crash can be seen when interface configuration is added using API and some Junos application (such as vrrpd, jdhcpd etc) send configuration for the same interface using Overlay files. This is because, in dcd the internal data structures are not updated correctly when config source is changed from API to Overlay which eventually leads to corruption. It does not cause any service impact.
1757801	High memory utilization is observed on all Junos platforms Product-Group=junos Severity=Major	On all Junos platforms, the device control daemon (dcd) consumes some memory when a new configuration related to any protocol is added and it is not freeing up the memory. This resulted in a high dcd memory utilization.
1757936	Services using the management interface will be affected on all Junos platforms Product-Group=junos Severity=Major	On all Junos platforms, the default management IFL (unit 0) and IFF (ethernet-switching/vpls) will not be created when management IFL (Logical Interface) is configured to get address from DHCP and when user provided management IFL configuration is deleted.
PR Number	**Synopsis**	**Category: Firewall Filter**
1697959	Deactivating and activating the GRES causes churn in dfwd filter addition/deletion Product-Group=junos Severity=Major	On all Junos dual-RE platforms, when performing activate/deactivate Graceful Routing Engine Switchover (GRES) multiple times synchronization issues are observed between the master and backup dfwd process.
1749092	High CPU utilization of the mib2d process will be observed with error messages due to stale SNMP requests Product-Group=junos Severity=Major	On all Junos platforms, high CPU utilization, up to 100%, of the mib2d process will be observed with error messages and this may also result in a crash/core when memory gets exhausted due to a gradual increase in stale SNMP (Simple Network Management Protocol) requests.
PR Number	**Synopsis**	**Category: ACX platform interface issues**
1747140	QSFP interfaces show additional flap during PFE bringup Product-Group=junos Severity=Major	On Junos ACX5448 platform, the QSFP (Quad Small Form-factor Pluggable) interfaces can possibly see a momentary flap during device or pfe bring up.
PR Number	**Synopsis**	**Category: ACX IFL, IFF creation**
1764083	Interface flaps leading to PFE crash due to FPC heap corruption Product-Group=junos Severity=Major	Frequent interface flaps will lead to the PFE (Packet Forwarding Engine) crash. This issue is seen because two threads simultaneously access the same memory location.
PR Number	**Synopsis**	**Category: EVO Class of Services**
1766873	Duplicate code points through code-point-aliases under a classifier results in cosd crash Product-Group=junos Severity=Major	On all Junos Evolved platforms, the class-of-service (COS) commit validation is missing for classifier when using code-point-aliases. Configuring duplicate code-point-aliases and using them in a classifier will result in the cosd crash. The system can be recovered by correcting the config and applying the "restart class-of-service" command.

PR Number	Synopsis	Category: EVO L2 Control Plane PRs
1740561	Traffic loss is seen due to anomalies after the recreation of IFLs Product-Group=junos Severity=Critical	On all Junos Evolved Platforms, in the EVPN-VXLAN DCI (Data center Interconnect) scenario, traffic loss is seen due to anomalies when any catastrophic interface change is done which results in the IFL (logical interface) deletion and recreation by the system.
1743744	Junos OS and Junos OS Evolved: The l2ald crashes on receiving telemetry messages from a specific subscription (CVE-2024-30402) Product-Group=junos Severity=Critical	An Improper Check for Unusual or Exceptional Conditions vulnerability in the Layer 2 Address Learning Daemon (l2ald) of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated, adjacent attacker to cause a Denial of Service (DoS). Please refer to https://supportportal.juniper.net/JSA79180 for more information.
1749191	Some of the MAC addresses are not learned in EVPN-VXLAN scenario Product-Group=junos Severity=Critical	On all Junos and Junos Evolved platforms configured with EVPN-VXLAN (Ethernet Virtual Private Network-Virtual Extensible Local Area Network) when network events such as interface flap/BFD (Bidirectional Forwarding Detection) flap etc. leads to overlay BGP (Border Gateway Protocol) / EVPN flap and results in VTEPs (VXLAN Tunnel Endpoint), IFLs (Logical Interface), IFFs (Interface Family) and IFBDs (Interface Family Bridge Domain) corresponding to remote MH (Multi Home) peers to be deleted and causes new ones to be recreated, it is observed that even though MAC address is received it is not being programmed which results in missing entries of MAC addresses in the MAC table.
1749745	The MAC learning process is impacted and l2ald gets stuck when scaled L2 services and telemetry are configured Product-Group=junos Severity=Major	On all Junos Evolved platforms having scaled L2 (Layer 2) services and telemetry is enabled, under a rare scenario, it is seen that the l2 daemon is getting stuck due to which the show commands served by l2ald are not working and MAC (Media Access Control) addresses are not getting learned which leads to traffic drop.
1769086	Data center interconnect configuration addition needs to be non-catastrophic. Product-Group=junos Severity=Major	Adding interconnect configuration can be catastrophic behaviour which means BD (Bridge domain) and routing instance object will be deleted and added back, during this window there will be traffic drop.
PR Number	**Synopsis**	**Category: mgd, ddl, odl infra issues**
1752374	Subsequent commits hang will be seen, when transfer-on-commit fails Product-Group=junos Severity=Major	On all Junos Evolved platforms, When transfer-on-commit is configured and it fails as the destination is unreachable or invalid, commit lock taken by automatic rollback commit is not released. Due to this, subsequent commits result in a hung state.
1783888	[Junos OS Evolved] Traceoptions log sometimes shows UTC timestamp, although non UTC time-zone is configured Product-Group=junos Severity=Major	On all Junos OS Evolved platforms, traceoptions log sometimes shows UTC timestamp, although non UTC time-zone is configured.
PR Number	**Synopsis**	**Category: EVPN control plane issues**
1704286	The VPN traffic loss will be seen in EVPN-VXLAN scenario Product-Group=junos Severity=Major	On Junos and Junos OS Evolved platforms in a type 5 EVPN -VXLAN scenario with GR (Graceful Restart) enabled when rpd is restarted on a PE (Provider Edge) device that advertises prefixes in VRF.inet to other DCs (Data Centers) via EVPN type 5 route, the PE prematurely sends EOR (End-of-RIB) message to EVPN peers before it has learned all the VPN prefixes in a VRF. This results in traffic loss on EVPN peers until VPN prefixes are relearnt.
1717016	Interface related commits causing RPD CPU spike Product-Group=junos Severity=Major	On Junos and Junos OS Evolved platforms, any interface configuration change may cause RPD (routing protocol daemon) CPU spike on scaled configuration.
1722102	L2alm sends IPv6 NS with IRB link local address even though target IP is global address Product-Group=junos Severity=Major	On Junos and Junos Evolved platforms configured with EVPN-VXLAN, EVPN-MPLS, it is observed that L2alm sends IPv6 NS(Neighbor Solicitation) with link local address even through target IP is global address.

1732414	EVPN-VXLAN interconnection DCI forwarding problem was observed when one of the AGW IRB interfaces failed in data centers spine Product-Group=junos Severity=Major	On Junos platforms, using the Ethernet Virtual Private Network-Virtual extensible Local Area Network (EVPN-VXLAN) setup with active-active Anycast Gateway (AGW) within two different Data Centers (DCs), using DCI interconnect config with interconnect encapsulation Multiprotocol Label Switching (MPLS). On the spine routers dc1-spine1 and dc2-spine1 the same Integrated routing and bridging (IRB) AGW address is configured. There is one IRB interface per DC, DC1 (spine1 has irb, spine2 doesn't have and same for the DC2). When IRB interface failed in DC1/DC2 spine, the trigger of reprogramming same MAC received from DC2 missed as there is a separate macdb entry with vlan-id and VNI even if both are same Bridge domain (BD). Usually, it is expected to configure IRB on all Gateway (GW) nodes. If the user trying with IRB only on one GW node.
1734686	While doing a migration from VPLS to EVPN, when any changes are done like FPC restart or device reboot, the crash is observed Product-Group=junos Severity=Major	On all Junos platforms, After migration from VPLS (Virtual Private LAN service) to EVPN (Ethernet Virtual Private Network), when any catastrophic change or FPC (Flexible PIC Concentrator) is restarted, the crash is observed.
1747706	Intermittent packet loss can be observed in evpn-vpws local switching scenario Product-Group=junos Severity=Minor	When evpn-vpws local switching is configured, RPD is setting the user flags on the ccc ucast next hop, which is being interpreted as MPLS_OAM_FILTER and leading to traffic dropThe packet loss is random, the pattern is still to be analyzedThe issue can be seen regardless of control word and vlan configuration on the instance and interfaces
1761852	The rpd can crash on all Junos platforms in Seamless DCI scenario Product-Group=junos Severity=Major	On all Junos platforms, a crash can be seen for the rpd (routing process daemon) in EVPN (Ethernet Virtual Private Network) seamless DCI (Data Center Interconnect) scenario when the 'evpn interconnect' and the BD (Bridge Domain) configuration are deleted in the same commit. There will be traffic loss when the rpd crashes but the system will self-recover.
1764487	HIgh CPU in RPD due to evpn ip-move when large number of ip's learned on same MAC Product-Group=junos Severity=Major	The issue is caused due to large number of ip address being linked to a single mac entry. The evpn ip move changes were looping multiple times through each of the ip entries associated to the mac causing high CPU/Memory utilization in RPD.
PR Number	**Synopsis**	**Category: EVPN Layer-2 Forwarding**
1712259	The Anycast Gateway stretched across 2 DCs over the seamless MPLS stitching DCI does not have Anycast Gateway MAC information coming from the remote DC when VLAN and VNI ids are different Product-Group=junos Severity=Critical	On all Junos and Junos OS Evolved platforms, the AnyCast Gateway stretched across 2 Data Centres (DC) over the Data Centre Interconnect (DCI) using seamless Multiprotocol Label Switching (MPLS) stitching through Interconnect knob and having different VLAN and Virtual Network Identifier (VNI) ids (e.g., VLAN ID 101 <-- -> VNI 1101), then upon deactivating the Integrated Routing and Bridging (IRB) interface on all the gateways within DC, the AnyCast Gateway MAC information coming from Interconnect-Ethernet Segment Identifier (I-ESI) will not be available in the bridge mac-table and thus, the Inter VLAN/VNI routing will be impacted.
1718165	ARP learning issues are observed post-execution of the CLI command 'clear bridge mac-table' or 'clear ethernet-switching table' in the EVPN-MPLS over IRB environment Product-Group=junos Severity=Major	On all Junos and Junos Evolved platforms, L3 (Layer 3) traffic will be impacted when ARP (Address Resolution Protocol) entries get deleted for the MAC (Media Access Control) address having a bad state post execution of the CLI 'clear bridge mac-table' or 'clear ethernet-switching table' command in the EVPN-MPLS (Ethernet VPN - Multiprotocol Label Switching) over IRB (Integrated routing and bridging) environment.
1743913	IRB reachability issues may be observed in the EVPN-VXLAN environment when looped ARP comes on ESI-LAG Product-Group=junos Severity=Major	On Junos and Junos OS Evolved platforms (except MX platforms) with EVPN-VXLAN (Ethernet VPN - Virtual Extensible LAN) configured, in case of traffic loop conditions, self-generated ARP packets (having physical-IRB MAC as SMAC) may come back to the same node where it originated. Such rare scenarios, when the MAC address of the IRB (Integrated Routing and Bridging) ages out and is cleared from the MAC table, also associated MAC-IP route (IRB route) might get cleaned. This may result in IRB reachability issues as the remote VTEPs (Virtual Tunnel End Point) won't have IRB information of the local VTEP and on the local VTEP, there won't be EVPN database entry and type-2 EVPN advertisements for local IRB towards the remote VTEPs.
1751386	Re-ARP is not sent before MAC entry expires in EVPN environment on Junos MX platforms Product-Group=junos	On Junos MX240, MX304, MX480, MX960, MX2010, MX2020, MX10004, MX10008 platforms with MPC10/MPC11/LC9600 line cards, Re-Address Resolution Protocol (Re-ARP) is not sent before Media Access Control (MAC) entry expires. It causes a

	Severity=Major	service impact in Ethernet Virtual Private Network- Virtual eXtensible Local-Area Network (EVPN-VxLAN) scenario with IRB (Integrated Routing and Bridging) and BD (Bridge Domain) configured.
1758677	MAC addresses programming failure resulting in traffic flooding Product-Group=junos Severity=Major	Issue 1: On QFX5K and EX platforms in the VXLAN (Virtual Extensible LAN) environment, traffic flooding will be observed for MAC addresses not getting programmed in the hardware with VPLAG (Virtual Chassis Port Link Aggregation) configured and BGP (Border Gateway Protocol) flaps. This issue happens when hardware programming by L2ALM to PFE fails, and during re-sync, SVLBNH (shared VXLAN load balancing next hop) info is not sent to PFE/hardware. Issue 2: On all Junos and Junos Evolved platforms, l2alm sends a delete request for control MAC addresses to l2ald after multiple hardware sync failures.
1770407	The l2ald crash will be seen in EVPN-MPLS scenarioo Product-Group=junos Severity=Major	On all Junos and Junos OS Evolved platforms with EVPN-MPLS configured, when a BD(Bridge Domain) is not included in "vnid-list" of EVPN-MPLS(Ethernet Virtual Private Network with Multiprotocol Label Switching) routing instance and router-id is deleted, the l2ald process will crash. There is no service impact due to this issue.
1773734	Traffic flooding is observed due to MAC-IP deletion by l2alm in the EVPN-VXLAN / EVPN-MPLS environment Product-Group=junos Severity=Major	On Junos and Junos Evolved platforms, in the EVPN-VXLAN (Ethernet VPN-Virtual Extensible LAN) / EVPN-MPLS (Ethernet VPN-Multiprotocol Label Switching) environment when l2alm (Layer 2 Address Learning Manager) deletes the MAC-IP (Media Access Control - Internet Protocol Address) entry but doesn't re-add the MAC-IP entry right away leads to traffic flooding i.e. might result in congestion, packet looping, and packet drops.
PR Number	**Synopsis**	**Category: Control plane EVPN multicast**
1738355	Multicast will not work if one or more VLANs are removed from the interface having multicast configured Product-Group=junos Severity=Critical	On all Junos QFX5K and EX4K platforms with igmp-snopping configured, if one or more VLANs are removed from the interface having Multicast configured results in Multicast will not work. The issue happens in the EVPN-VxLAN (Ethernet VPN - Virtual Extensible LAN) environment with Multicast configuration.
1758171	Junos OS and Junos OS Evolved: Receiving specific traffic on devices with EVPN-VPWS with IGMP-snooping enabled will cause the rpd to crash (CVE-2024-39514) Product-Group=junos Severity=Major	An Improper Check or Handling of Exceptional Conditions vulnerability in the Routing Protocol Daemon (rpd) of Juniper Networks Junos and Junos OS Evolved allows an unauthenticated, adjacent attacker to cause a Denial of Service (DoS). Please refer to https://supportportal.juniper.net/JSA82980 for more information.
PR Number	**Synopsis**	**Category: EX4100 PFE**
1744190	Virtual Chassis formation will not happen automatically on all EX platforms except EX4400 after zeroize Product-Group=junos Severity=Critical	Virtual Chassis members are not forming Virtual Chassis on all EX platforms except EX4400 due to cross connection of VC links in specific ring topology setup after zeroize. Each device will function as standalone.
1752756	L2ALD_IFBD_COUNT_EXCEED is not generated when exceeded max number of vmember Product-Group=junos Severity=Major	On EX4100 platform, there is no log for" L2ALD_IFBD_COUNT_EXCEED " even though exceeded max number of vmember.
1770448	[EX46/QFX5K]MTU Errors are counted when receiving packets up to 4 bytes in MTU Product-Group=junos Severity=Major	When receiving packets from MTU + 1 bytes to MTU + 4 bytes on L2 interfaces, packets is transmitted. but MTU errors are counted
PR Number	**Synopsis**	**Category: EX4100 RE, Platform Infra, Drivers**
1747277	Soft OIR of the link connected to 10GBASE-T SFP will not update the link state at the other end Product-Group=junos Severity=Minor	On EX4400, EX4100, and QFX5120-48Y platforms, soft Online Insertion and Removal (OIR) of the link connected to 10GBASE-T Small Form-Factor Pluggable (SFP) will not disable the transmission on JNP-SFPP-10GE-T transceiver and the link state of the other end will not be updated. False link state could lead to service impact.
PR Number	**Synopsis**	**Category: EX4400 PFE software**

1757160	Multicast traffic may be dropped if both bpdu-block-on-edge and igmp-snooping are configured. Product-Group=junos Severity=Major	On EX2300, EX3400, EX4300MP, EX4100, and EX4400 Platforms in a Virtual Chassis (VC), multicast traffic in the Local Network Control Block (224.0.0.0/24) may be dropped on VC ports if both bpdu-block-on-edge and igmp-snooping are configured.
1757329	The dcpfe process crash will be seen when L2PT interfaces are configured with multiple protocols Product-Group=junos Severity=Major	On QFX5K Junos/EX4650/EX4600/EX4400/EX4100/EX4300MP platforms that support Layer 2 protocol tunneling (L2PT), sending the bi-directional traffic on those interfaces and deleting/re-adding the L2PT multiple times causes the dcpfe crash which triggers Packet Forwarding Engine (PFE) restart.
1757431	Whenever IGMP leave request is initiated by receiver unicast traffic to the host IP on the switch port is non-responsive Product-Group=junos Severity=Major	On Junos EX series and QFX5K platforms, having VC (virtual-chassis) when IGMP (Internet Group Management Protocol) snooping is enabled and when there is an mrouter (multicast router) interface present in a non master VC (virtual-chassis) member, IGMP leave packets are sent back to the source interface which impacts the unicast traffic of the end host.
1759821	The configuration was not applied correctly to set the transmit-rate to the same speed as the interface speed Product-Group=junos Severity=Major	On 1G port if tx rate is applied with 4m(Q0) + 996m (Q1). Config is failed in COSD with the following log and not get pushed to PFE. COSD_TX_QUEUE_RATES_TOO_HIGH: cos_validate_scheduler_shaper_conflict:820 : Unable to apply scheduler map CPE-Transmit-VPN1G-normal-only to interface ge-x/x/x: sum of scheduler transmission rates exceeds interface shaping or transmission rate
1760229	The fxpc process crashes and causes a traffic loss when adding and deleting IRB configuration Product-Group=junos Severity=Major	Traffic loss will be seen on all Junos and Junos OS Evolved platforms when performing IRB (Integrated Routing and Bridging) configuration modifications. When the issue occurs, the fxpc process crashes and generates crash files.
1761220	The 'input-vlan-map push' operation will not work on double-tagged frames Product-Group=junos Severity=Major	On Junos EX/QFX5120 platforms with QinQ setup packets with multicast payloads such as OSPF (Open Shortest Path First)/ISIS (Intermediate. System to Intermediate System), when 'input-vlan-map push' is configured to push an outer VLAN (Virtual Local Area Network) tag on to a double-tagged frame, the egressing frame will be tagged incorrectly. Instead of a push operation, the outer VLAN tag of the ingressing double-tagged frame will be swapped and sent out. This results in unexpected behavior or traffic loss as such protocol packets will not have the expected VLAN tag information.
1764085	LLDP neighborship is not forming in non-master members Product-Group=junos Severity=Major	On Junos QFX and EX platforms, with EVPN VXLAN configured in VC topology, LLDP BPDUs are sent tagged out of remote FPC ports which are member of VXLAN enabled VLAN.
1771111	EX4100/4400 : Error message 'COS default: IEEE 802.1ad defaults not specified' upon commit operation. Product-Group=junos Severity=Major	On EX4100 and EX4400 series switch, error message 'COS default: IEEE 802.1ad defaults not specified' might be observed on commit operation.
1771222	Dynamic VLAN change on one port is affecting forwarding plane traffic on other ports to which no changes were done Product-Group=junos Severity=Major	On QFX and EX platforms, if dot1x is enabled, when dynamic VLAN configuration in the radius server is changed and restored for one port, forwarding plane traffic would be affected on other ports to which no changes were done.
1790316	The access port is dropping a VLAN-tagged packet of which the interface is a VLAN-member Product-Group=junos Severity=Major	On all Junos EX and QFX5K platforms supporting Virtual Extensible LAN protocol (VXLAN), the access ports drop Virtual Local Area Network (VLAN) tagged traffic of the same VLAN for which the interface is configured. Though ideally, the access port should be accepting only untagged traffic, because of customer requests the access ports were made to accept tagged packets of which the interface is a VLAN member along with untagged traffic.
PR Number	**Synopsis**	**Category: EX4400 platform**
1682097	Beacon led is not working on EX platforms Product-Group=junos Severity=Major	All beacon LEDs on the specified FPC does not turn on after a request command.
1709483	On EX4400, "show chassis environment power-supply-	On EX4400, "show chassis environment power-supply-unit" displays only master

	unit" displays only master member's details. Product-Group=junos Severity=Major	member's details.
1729464	While exporting telemetry data, transceiver data is also streamed when there is no transceiver in device itself. Product-Group=junos Severity=Major	When data is streamed through telemetry, transceiver data is also streamed, even when there is no transceiver in device itself. There is no functional impact. There is no workaround for this issue.
1731146	On EX4400, PIC2 details may not be not displayed for "show snmp mib walk entPhysicalVendorType" output Product-Group=junos Severity=Major	On EX4400, PIC2 details are not displayed for "show snmp mib walk entPhysicalVendorType" output, when PIC2 is present.
1731225	EX4400 platforms will not boot from USB if the device had booted earlier without a USB plugged in Product-Group=junos Severity=Major	On EX4400, If media USB is inserted after device is booted, BIOS will not have its entry in boot device list. To have USB entry in boot device list need to reboot once with inserted USB and then next reboot with "request system reboot usb ".
1735786	Port LEDs are not working as expected when the mode is changed from default to EN Product-Group=junos Severity=Critical	On EX4400, Show chassis LED output for EN mode does not display the physical LED status correctly- Physical LED functionality works as expected.
1737500	On EX4400, request system halt/power-off doesn't turn off FAN LED's Product-Group=junos Severity=Major	On EX4400, request system halt/power off CLI doesnt turn off rear FAN LEDs.
1741724	1G uplinks on EX4400 with pre-existing configuration do not come up after 4X10G ULM insertion Product-Group=junos Severity=Major	On Junos EX4400 platforms, pre-configured 1G ports do not come up after 4X10G ULM (Universal Link Module) insertion event.
1742114	Basic VLAN configuration on EX2300-24MP / EX2300-48MP / EX4400-24MP / EX4400-48MP is missing from factory default configuration Product-Group=junos Severity=Major	On EX2300 and EX4400, on CLI "load factory-default", config loaded does not have VLAN configuration. This is present in the factory default config loaded after zeroize.
1751700	Incorrect egress MTU errors when larger than 1500 byte packets are sent on L2 ports Product-Group=junos Severity=Major	On Junos EX4100 and EX4400 Platforms, incorrect egress MTU errors seen when larger than 1500 byte packets are sent on L2 ports. There is no functionality impact only MTU Error counters incrementing.
1754548	EX4400 Virtual Chassis has boot-up issues Product-Group=junos Severity=Major	EX4400 could be stuck during boot, when one end of the twisted pair cable is connected to the primary console port and the other end is left unconnected/dangling.
1754931	The transceiver fails to get detected after the system reboot Product-Group=junos Severity=Major	On certain EX platforms, when the device is rebooted, transceivers will not be detected. Failing to detect the transceiver results in no IFD.
1759351	EX4400:PSM is not detected in "show chassis hardware" until AC feed is connected to it Product-Group=junos Severity=Major	The Power Entry Module (PEM) after insertion will not be detected/displayed in the show chassis hardware CLI output , until the power feed is connected .
1773103	TDR link status not consistent in CLI Product-Group=junos Severity=Major	Link status is different from " show diagnostics tdr" and " show diagnostics tdr interface XXX" output.
PR Number	**Synopsis**	**Category: PFE EVPN / VxLAN related issues on EX platforms**
1746998	VLAN traffic received over VTEP is being dropped Product-Group=junos	On Junos VC (EX and QFX) platforms, packets coming on VTEP (VXLAN tunnel endpoint) from the core are not sent out when restarting of VC with VxLAN

	Severity=Major	configuration.
1774202	The DHCP client will not be able to get the IP address Product-Group=junos Severity=Major	On Junos EX4300MP platforms, in the Virtual Extensible LAN Layer 3 Gateway (VXLAN L3GW) environment with Dynamic Host Configuration Protocol (DHCP) security configured, the offer packets going towards client-facing interfaces are coming out with an additional vlan tag due to which DHCP bindings will not work.
1776539	VXLAN traffic from remote VTEP with GBP Extension flag is dropped on all Junos EX4400 and QFX5120 platforms Product-Group=junos Severity=Major	VXLAN (Virtual Extensible Local Area Network) encapsulated packets with G-bit set, received from remote VTEP (Virtual Tunnel End Point) are dropped on all Junos EX4400 and QFX5120 platforms. VXLAN traffic is getting dropped when it is received from remote VTEP with GBP (Group Based Policy) Extension flag and is destined to a downstream port which is authenticated using dot1x single-secure or multiple supplicant mode.
PR Number	**Synopsis**	**Category: EX Entry Level Access VC platform**
1740064	The interface speed is not updated during reboot on Junos EX platforms Product-Group=junos Severity=Major	
PR Number	**Synopsis**	**Category: Express PFE including evpn, vxlan**
1677422	QFX10000 series platforms generates error messages constantly and IPv6 routing is not performed when configured rpf-check and inet6 on VXLAN enabled interface and trying to resolve arp ndp Product-Group=junos Severity=Major	With rpf-check (enabling reverse-path forwarding) and ipv6 configured on VXLAN (Virtual Extensible LAN) enabled interface, trying to resolve arp ndp nexthop, error messages are constantly observed and ipv6 routing failed. For the ipv6 routes which point to the IPv6 ndp (Neighbor Discovery Protocol) nexthop, the fdb entry needed more space than the allocated space. As a result, PFE was unable to add this entry into fdb and IPv6 routing was not performed.
1779890	On QFX10002-60c platforms, during system reboot and fpc reboot time, some non functional error logs are displayed. Product-Group=junos Severity=Major	On QFX10002-60c express based Junos platform the error logs are seen during boot time. These errors are not impacting any functionality. The table is getting programmed correctly. These are seen during system reboot and fpc reboot time. We will be emitting the logs for non default routing instances and not for default routing instance.
PR Number	**Synopsis**	**Category: Express PFE L2 fwding Features**
1723433	QFX10K not bridging multicast traffic with TTL=1 on same VLAN Product-Group=junos Severity=Major	On Junos QFX10K platforms, when PIM is enabled on the IRB (Integrated Routing and Bridging) interface and multicast traffic with TTL=1 (Time-to-live) needs to be L2 switched in the same BD (Bridge Domain), it gets discarded as TTL was trying to be decremented even for Layer 2 switching.
1738197	Blackholing of l3-inject traffic on QFX10K platforms Product-Group=junos Severity=Major	On Junos QFX10K platforms, because of any hardware (HW) or chassis management (CM) issue there will be Trinity Offload Engine (TOE) cmerrors. Some cmerrors are classified as MAJOR and the default action for these errors is cmalarm but it will halt the Packet Forwarding Engine (PFE) TOE HW. Due to which PFE is not able to forwards packets to the Application-Specific Integrated Circuit (ASIC) even though it is active and can forward packets.
1739258	The ksyncd process crash would be seen on backup RE Product-Group=junos Severity=Major	On QFX10008 and QFX10016 platforms with IRB(Integrated Routing and Bridging), EVPN-VxLAN(Ethernet VPN-Virtual Extensible LAN) and enhanced-arp feature enabled, high availability will be impacted as backup RE(Routing Engine) will remain down due to ksyncd (kernel synchronization process) failure. In case of switchover, if backup become the new master, then traffic drop will happen.
1746435	QFX10002-60c port et-0/0/30 part of a lag is dropping peer ARP reply after configuring a GRE tunnel Product-Group=junos Severity=Major	GRE IFL configuration was changing the physical port's igport attributes in IGP.
1748500	Traffic drop will be observed when Label MPLS traffic egressing out on the IRB interface as IPV4 Product-Group=junos	On QFX10K platforms, Label MPLS (Multiprotocol Label Switching) (labeled-unicast) traffic egressing out on IRB (Integrated routing and bridging) interface as IPV4 traffic can get dropped.

	Severity=Critical	
1770678	Incorrect IFL value resulting in the PFE crash Product-Group=junos Severity=Major	On Junos QFX10K platforms, the PFE crash is observed resulting in traffic loss due to an incorrect IFL (Logical Interface) value while static MAC address programming.
1771879	The IP packet of L2 Unicast MAC and L3 undirected broadcast IP (255.255.255.255) is dropped when sent over an IRB interface Product-Group=junos Severity=Major	On certain Junos QFX platforms, when an IP packet with L2 Unicast destination MAC and L3 undirected broadcast destination IP is received on an IRB (Integrated Routing and Bridging) interface, then the packet is dropped.
1779527	At the interface level, only half of the traffic is policed when applying a policer Product-Group=junos Severity=Major	On QFX10002-36q, QFX10002-72Q, QFX10008 and QFX10016 platforms, when applying a policer at the interface level only half of the traffic is policed.
PR Number	**Synopsis**	**Category: Express PFE L3 Multicast**
1756923	A heap memory leak will be seen when P2MP LSP MBB events happened Product-Group=junos Severity=Major	On PTX3000 and PTX5000 platforms, nodes having Point-to-MultiPoint (P2MP) MPLS label switched path (LSP) passing through them will show a slow increase in Flexible PIC Concentrators (FPC) heap memory utilization when there are P2MP LSP Make-Before-Break (MBB) events happened and when adaptive load balancing (ALB) is enabled on the aggregated ethernet (AE) interface. FPC may crash if the memory leak persists for an extended period.
PR Number	**Synopsis**	**Category: Enhanced Broadband Edge support for firewall**
1719427	The subscribers will be stuck in a terminated state when an FPC is taken offline Product-Group=junos Severity=Major	On MX platforms, If a Flexible PIC Concentrator (FPC) is taken offline while it has Broadband Edge (BBE) subscribers over it, due to timing issues a few subscribers state on the FPC may not get properly cleaned up and will be stuck in a terminated state. This can adversely affect subsequent subscriber logins which fail with an "orphaned filter" error.
PR Number	**Synopsis**	**Category: SRX4100/SRX4200 platform software**
1630981	IPSec VPN traffic might get dropped on SRX4100/SRX4200 Product-Group=junos Severity=Minor	All VPN traffic may internally drop during encryption / decryption processing in HW engine requiring PFE plane reset.
1761668	False SNMP traps for power supply unit failure generated on SRX4100 and SRX4200 platforms Product-Group=junosvae Severity=Major	On SRX4100/SRX4200 platforms, false SNMP traps for power supply unit failure generated as instability with the transmission in the hardware.
PR Number	**Synopsis**	**Category: Libjtask for RPD tasks, scheduler, timers, memory, and slip**
1692738	On all Junos lsys systems RPD process crashes due to JET client invoking rpc handled by RPD daemon Product-Group=junos Severity=Critical	RPD process crash might be seen when the gRPC stack expects a 8 byte aligned memory but gets a 4 byte aligned memory instead.
1724986	With BGP traceoptions configuration high CPU utilization will be observed and the rpd process may crash Product-Group=junos Severity=Minor	On all Junos and Junos Evolved platforms BGP traceoptions configuration will have an impact on the CPU, threads will be busy and will take time to recede in spite of disabling it. It is important we enable a specific trace flag and disable it when the CPU goes high. It is also important not to perform switchover and other triggers which can add load to the CPU during traces are enabled. Traces must be enabled discretely.
PR Number	**Synopsis**	**Category: MX Inline Jflow**
1716505	Memory initialization of large blocks causes traffic congestion in PFE or feature configuration fails	Memory initialization of large blocks of PFE (Packet Forwarding Engine) memory such as hash table initialization expands memory which fails due to over-

	Product-Group=junos Severity=Major	utilization and causes traffic congestion or feature configuration failure.
PR Number	**Synopsis**	**Category: Fast Ethernet interfaces**
1707707	Physical link remains stuck in down state on certain MX platforms Product-Group=junos Severity=Major	On Junos MX240/MX480/MX960/MX2008/MX2010/MX2020 platforms having MPC10E/MPC11E line cards, when link monitoring with auto recovery of PFE (Packet Forwarding Engine) is configured, after introduction of bit errors the link goes down and is supposed to come up after disabling the link monitoring knob. But it has been observed that the physical link remains down.
PR Number	**Synopsis**	**Category: Kernel software for AE/AS/Container**
1698781	The kernel crash can be seen in the VPLS scenario Product-Group=junos Severity=Major	On Junos platforms, Kernel crashes can happen in VPLS (Virtual Private LAN Service) scenario. This issue is seen when the VPLS has IRB (Integrated Routing and Bridging) interface and the next-hop of IRB is RLT (Redundant Logical Tunnel) interface. This issue is triggered when there is an ARP request sent from the IRB interface. There can be a service impact because of this issue as the device can reboot.
PR Number	**Synopsis**	**Category: IoT data filtering/streaming**
1745089	Security-metadata-streaming dynamic-filter not submitting data for IoT device traffic Product-Group=junos Severity=Major	On all Junos NFX and SRX platforms, sw-iot (Sensor Web and Internet of Things) functionality will not work when there are HTTP (Hypertext Transfer Protocol) and DNS (Domain Name System) features configured under security-metadata-streaming along with dynamic-filter.
PR Number	**Synopsis**	**Category: Integrated Routing & Bridging (IRB) module**
1629345	Inter vlan ipv6 traffic loss for some hosts after configuration remove and restore. Product-Group=junos Severity=Major	For a topology with VSTP and VRRP configured and IPV6 traffic, if VSTP bridge priority is changed a couple of times (to trigger toggling of root bridge), it is possible that V6 traffic drop is seen on some of the streams.
PR Number	**Synopsis**	**Category: ISIS routing protocol**
1713008	Stale entries present in the lsdist table after ISO address change Product-Group=junos Severity=Major	On all Junos and Junos OS Evolved platforms configured with IS-IS and MPLS traffic engineering database (TED), if there is an ISO address change on another Intermediate System (IS), there will be stale entries being present in the link-state distribution (lsdist) table even though they might have been deleted in IS-IS and TED. This has an impact on the routes, and thus the services, related to the stale entries present in the lsdist.
1738222	RPD crashes when multiple ISIS processes are configured Product-Group=junos Severity=Major	On all Junos and Junos Evolved platforms, RPD crash files are seen during the GRES (graceful restart) event as GRES functionlity is not supported in protocol isis-instance <>.
1752551	Traffic drop is seen if chained-composite-next-hop is turned on for Segment Routing Product-Group=junos Severity=Major	On all Junos and Junos Evolved platforms, Traffic drop is seen if chained-composite-next-hop is turned on for Segement Routing ISIS because backup path is programmed as a POP in Composite-next-hop (CNH) and Push in Forwarding-next-hop (FNH).
1753003	The rpd crashes on all Junos and Junos Evolved platforms with IS-IS, segment routing and flex algo configured Product-Group=junos Severity=Major	On all Junos and Junos Evolved platforms, with IS-IS, segment routing and flex algorithm enabled, when the route from ribgroup is deleted due to interface flap, it leads to crash of the infra module as route entry table does not match with the rtbit table (which is passed from IS-IS).
1778841	With protocol ISIS configured, any new LSP generation triggers SPF Product-Group=junos Severity=Major	On all Junos platforms, with ISIS configured, when commit or any operation that attempts for LSP generation, an SPF is triggered.
1782887	Traffic blackhole due to Flex-algo not removing stale	On all Junos and Junos Evolved platforms, in an ISIS scenario using Flex-algo ,

	entries from ISIS database Product-Group=junos Severity=Critical	the system does not remove the stale (outdated) entries from the ISIS database causes traffic blackholing. This issue could lead to some traffic loss, as the routing information stored in the ISIS database does not get properly updated.
PR Number	**Synopsis**	**Category: track re issu control procedure bugs**
1740744	ISSU doesn't break if INDB crashes Product-Group=junos Severity=Major	On Junos platforms, when ISSU (in-service software upgrade) is initiated, a process called INDB (Incompatible Database) will be triggered to perform a pre-check on database compatibility. There could be some corner case that causes the INDB crash. If that happens, the ISSU should be aborted.
PR Number	**Synopsis**	**Category: jdhcpd daemon**
1694952	Auto-image-upgrade knob is not present when EX-VC is zeroized and VC is formed Product-Group=junos Severity=Major	When EX series VC (Virtual Chassis) members are zeroized or if it is powered on for the first time after halt, "set chassis auto-image-upgrade" configuration is not configured during the process of ZTP (Zero-touch Provisioning) flow and VC formation. Absence of this configuration will not allow user to download configuration and images via ZTP.
1706709	Junos OS: jdhcpd will hang on receiving a specific DHCP packet (CVE-2023-36842) Product-Group=junos Severity=Major	An Improper Check for Unusual or Exceptional Conditions vulnerability in Juniper DHCP Daemon (jdhcpd) of Juniper Networks Junos OS allows an adjacent, unauthenticated attacker to cause the jdhcpd to consume all the CPU cycles resulting in a Denial of Service (DoS). Please refer to https://supportportal.juniper.net/JSA75730 for more information.
1743611	DNS received through DHCP is lost after a commit and not able to ping internet Product-Group=junos Severity=Critical	If name-server information is changed via CLI after the DHCP subscribers are up, DNS obtained from DHCP server is overwritten by local config. This may result in DNS look up failures in some cases.
1747800	Name-server resolution failure may be seen intermittently after zeroize or loading factory default config Product-Group=junos Severity=Major	On all Junos platforms, name-server resolution failure may be seen intermittently after zeroize or loading factory default config.
1752804	Delay in getting IP through DHCP cause traffic loss Product-Group=junos Severity=Major	On all Junos and Junos Evolved platforms, DHCP IP negotiation will be delayed due to inform processing at Junos relay, when a client sends inform message to server and DHCP server doesn't respond with inform ack message and the client immediately does DORA to obtain IP.
1764483	High CPU utilization for bbe-smgd process in the BNG scenario Product-Group=junos Severity=Major	On MX platforms in the Subscriber Management scenario with DHCP (Dynamic Host Configuration Protocol) ALQ (Active Leasequery) and 'no-advertise-routes-on-backup' configured, bbe-smgd high CPU utilization will be observed which can result in such as pfed crash, and FPC not coming online when the subscriber's sessions stacked over the PS (Pseudowire Subscriber) interface are not getting empty leading to an endless loop. The issue happens when a switchover from backup to master BNG (Broadband Network Gateway) device involving the transition of PS interface and route operation (ADD or DELETE) is performed.
1769598	The jdhcpd prcoess crash will be observed due to double free of memory allocation when DHCP ALQ is configured Product-Group=junos Severity=Major	On MX platforms , when DHCP ALQ (Dynamic Host Configuration Protocol Active Lease Query) is configured and subscriber management is enabled, the jdhcpd process crash will be observed due to double free of memory allocation. The DHCP services will be down and it will restore once jdhcpd process is restarted.
PR Number	**Synopsis**	**Category: JFlow bug tracker for SRX platforms**
1749830	SPC3 PIC crash Product-Group=junos Severity=Major	SPC3 PIC will crash when the SPU is in dedicated Cp mode "SPU Cp" and Jflow information is queried by vty command. This fix will prevent jflow related queries from vty when the SPC3 SPU is in dedicated CP mode and jflow is initialized on SPU ins this mode.
PR Number	**Synopsis**	**Category: jl2tpd daemon**
1720994	L2TP tunnels may time out if creation of bbe-smgd core	In a subscriber-management environment, L2TP tunnels may time out if bbe-

	dump takes a long time. Product-Group=junos Severity=Major	smgd crashes with core dump if creation of the core dump takes longer than the effective L2TP timeout.
PR Number	**Synopsis**	**Category: Adresses ALG issues found in JSF**
1750148	Junos OS: SRX5000 Series with SPC2: Processing of specific crafted packets when ALG is enabled causes a transit traffic Denial of Service (CVE-2024-30405) Product-Group=junos Severity=Critical	An Incorrect Calculation of Buffer Size vulnerability in Juniper Networks Junos OS SRX 5000 Series devices using SPC2 line cards while ALGs are enabled allows an attacker sending specific crafted packets to cause a transit traffic Denial of Service (DoS). Please refer to https://supportportal.juniper.net/JSA79105 for more information.
PR Number	**Synopsis**	**Category: Application aware Quality-of-Service**
1720517	Junos OS and Junos OS Evolved: Multiple Vulnerabilities in CLI command (CVE-2023-44176) Product-Group=junos Severity=Critical	A Stack-based Buffer Overflow vulnerability in the CLI command of Juniper Networks Junos OS allows a low privileged attacker to execute a specific CLI commands leading to Denial of Service. Repeated actions by the attacker will create a sustained Denial of Service (DoS) condition. Please refer to https://supportportal.juniper.net/JSA73140 for more information.
PR Number	**Synopsis**	**Category: Flow Module**
1692559	High latency and packet drops will be observed with the "transmit-rate exact" knob enabled for one or more schedulers of an IFL/IFD Product-Group=junos Severity=Major	On SRX1500, SRX4100, SRX4200, vSRX and NFX platforms, when one or more schedulers of an IFL/IFD queue have the knob "transmit-rate exact" enabled and shaping globally disabled, the packets start getting queued for the shaping disabled queue, and the backpressure verification is being ignored on the fast path processing. Now, if the shaping-enabled queue receives packets after idling for a long time, this will result in large numbers of packets getting enqueued at the egress queue and depletion of Memory Buffer (mbufs), leading to high latency and packet drop.
1755181	Traffic loss is observed for the existing session if there is an update for the next-hop MAC address Product-Group=junos Severity=Major	On SRX5000 series and SRX4600, for flow sessions that are using Express Path (a.k.a. Service Offload), the next-hop MAC address is not updated for existing sessions, when the Address Resolution Protocol (ARP) table entry for the next-hop IP address changes, as a result, traffic is stalled for those existing sessions. This may for example occur on Virtual Router Redundancy Protocol (VRRP) failovers of directly connected routers if they do not use a virtual MAC address or server load balancers failing over the VIP to a new device with a different MAC address. Note that from Junos 21.2 onwards, Express Path is enabled by default.
1756972	CPU utilization calculation is inaccurate on vSRX platform Product-Group=junos Severity=Major	On vSRX platform, when PowerMode IPsec (PMI) is enabled, the CPU displays less utilization compared to the actual utilization value.
1758208	Buffer leak when PMI sends out packet on egress interface with MTU smaller than the packet length Product-Group=junos Severity=Major	On all SRX platforms, when the IPv4/IPv6 packet is larger than MTU of the interface, it leaks the memory buffer.
1760545	The srxpfe process crashes when interface attributes are modified Product-Group=junos Severity=Major	On Junos SRX platforms except for SRX3xx, the 'srxpfe' (packet forwarding engine) crash can be seen which causes traffic loss. This rare issue can be encountered while changing interface configuration with PMI (PowerMode IPsec) enabled.
1761891	Multicast packets of specific size between 663 - 676 bytes getting dropped Product-Group=junos Severity=Major	On SRX platforms, due to the incorrect size of memory allocated in mbuf (Memory Buffer) multicast packets of specific sizes between 663 - 676 bytes get dropped resulting in multicast traffic impact.
1771176	The GTPv2 create session response packets will get dropped Product-Group=junos Severity=Major	On all SRX5K platforms, the source port of the the create session response packet of the General Packet Radio Switching (GPRS) Tunneling Protocol (GTP) version 2 will be changed to as same as the destination port and will be denied by the policy resulting in create session response packets getting dropped.

1777565	Packet drops will be observed in GRE scenarios on SRX and vSRX platforms Product-Group=junos Severity=Major	On SRX and vSRX platforms, when Generic Routing Encapsulation (GRE) tunnels are configured, packet drops will be observed when packets enter to a tunnel.
PR Number	**Synopsis**	**Category: High Availability/NSRP/VRRP**
1540654	Both primary and secondary nodes in chassis cluster go into disabled state in HA link down scenario Product-Group=junos Severity=Major	In case of single control link on (SRX5400, SX5600, SRX5800) chassis cluster setup, when HA control link goes down, both nodes go into disable state due to fabric link still UP.
PR Number	**Synopsis**	**Category: interfaces and zones for junos js software**
1711729	The 'targeted-broadcast' feature will not work on some SRX platforms. Product-Group=junos Severity=Major	On SRX 1500, SRX4100, SRX4200 and SRX4600 based platforms running Junos, 'targeted-broadcast' feature will not work. As a result, features like wake-on LAN (WOL) which rely on targeted broadcast will be affected.
PR Number	**Synopsis**	**Category: Firewall Network Address Translation**
1702811	Junos OS: MX Series and SRX Series: Processing of a specific SIP packet causes NAT IP allocation to fail (CVE-2024-21616) Product-Group=junos Severity=Major	An Improper Validation of Syntactic Correctness of Input vulnerability in Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows an unauthenticated, network-based attacker to cause Denial of Service (DoS). Please refer to https://supportportal.juniper.net/JSA75757 for more information.
PR Number	**Synopsis**	**Category: Firewall Policy**
1783249	Security policies may go out of sync during ISSU Product-Group=junos Severity=Major	On all SRX platforms, performing ISSU (In-Service Software Upgrade) to or from an affected release can lead to policies going out of sync between control plane and forwarding plane. Affected releases are 19.4R3-S13, 20.4R3-S8/9/10, 21.2R3-S6/7; 21.4R3-S5/6; 22.2R3-S2; 22.4R3; 22.4R3-S1; 23.4R1. To recover, use the CLI command "request security policies resync".
PR Number	**Synopsis**	**Category: User Firewall related issues**
1755593	Users authenticated via captive portal experience a noticeable delay of atleast 2-5 mins Product-Group=junos Severity=Major	On all SRX platforms, the user-firewall configuration in policy with push-to-identity enabled may cause a delay in web-authenticating the users.
1758332	Junos OS: SRX Series and EX Series: Multiple vulnerabilities in J-Web can be combined to allow a preAuth Remote Code Execution (CVE-2023-36851) Product-Group=junos Severity=Critical	A Missing Authentication for Critical Function vulnerability in Juniper Networks Junos OS on SRX Series and EX Series allows an unauthenticated, network-based attacker to cause limited impact to the file system integrity and access confidential information. Please refer to https://supportportal.juniper.net/JSA72300 for more information.
PR Number	**Synopsis**	**Category: IPSEC/IKE VPN**
1731764	Traffic loss occurs on downgrade/upgrade to any release Product-Group=junos Severity=Critical	On MX204, MX10003, MX10008, MX10016, vSRX, SRX1500, SRX4100, SRX4200 and SRX4600 platforms, if the junos-ike package was installed, this package will be lost after a Junos upgrade. Then instead of iked, the default kmd will be used again for IPSec which will lead to mismatch of package and will cause loss in traffic.
1753782	IPSEC VPN tunnel flaps on all Junos OS SRX platforms when configuration is committed from MIST Product-Group=junos Severity=Major	On all Junos OS SRX platforms IPSEC (Internet Protocol Security) VPN (Virtual Private Network) tunnel re-establishes when the configuration is committed from MIST and the remote-identity type is ASN distinguished-name.
1765321	In chassis cluster setup after failover AAMW status will	On all SRX platforms in a chassis cluster setup, when IKE negotiation is

	remain in the Requesting server certificate validation state on the new primary node Product-Group=junos Severity=Major	dependent on the certificates and because of any reason the Certificate Revocation List (CRL) download fails on the secondary node and failover happens, then on the new primary node Public Key Infrastructure daemon (pkid) will have certification validation issues and the Advanced Anti-Malware (AAMW) status for control plane will remain in 'Requesting server certificate validation' state, impacting Internet Key Exchange (IKE) negotiation and the Internet Protocol Security (IPsec) traffic.
1773276	IPsec tunnels will not be established due to memory leak Product-Group=junos Severity=Major	On all SRX platforms, due to a memory leak (304 bytes) happening with every Diffie-Hellman (DH) key exchange operation, after some time when QuickAssist (QAT) crypto memory hits the maximum capacity, then the Internet Protocol Security (IPsec)tunnels will fail to establish the connection with peers.
1783738	The kmd/iked process crashes under rare circumstances Product-Group=junos Severity=Major	On Junos SRX/MX platforms, VPNs (Virtual Private Network) that employ the use of KMD (ipsec-key-management) or IKED (ike-key-management) may inadvertently crash while generating the random number used by IPSec services which can cause the device to become very busy.
PR Number	**Synopsis**	**Category: Security platform jweb support**
1747984	Junos OS: SRX Series and EX Series: Security Vulnerability in J-web allows a preAuth Remote Code Execution (CVE-2024-21591) Product-Group=junos Severity=Major	An Out-of-bounds Write vulnerability in J-Web of Juniper Networks Junos OS SRX Series and EX Series allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS), or Remote Code Execution (RCE) and obtain root privileges on the device. Please refer to https://supportportal.juniper.net/JSA75729 for more information.
1763260	Junos OS: SRX Series and EX Series: J-Web - unauthenticated access to temporary files containing sensitive information (CVE-2024-21619) Product-Group=junos Severity=Major	A Missing Authentication for Critical Function vulnerability combined with a Generation of Error Message Containing Sensitive Information vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an unauthenticated, network-based attacker to access sensitive system information. Please refer to https://supportportal.juniper.net/JSA76390 for more information.
1779376	Junos OS: SRX Series and EX Series: J-Web doesn't sufficiently sanitize input to prevent XSS (CVE-2024-21620) Product-Group=junos Severity=Major	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an attacker to construct a URL that when visited by another user enables the attacker to execute commands with the target's permissions, including an administrator. Please refer to https://supportportal.juniper.net/JSA76390 for more information.
PR Number	**Synopsis**	**Category: PFE infra to support jvision**
1772266	PFE component of /interfaces/interface/subinterfaces/subinterface/state/ sensor may send data with frequency higher than requested by the collector Product-Group=junos Severity=Major	In a scale configuration, PFE component may send data for "/interfaces/ interface/ subinterfaces/ subinterface/ state/" sensor with frequency higher than requested by the collector.
PR Number	**Synopsis**	**Category: Platform infra to support jvision**
1771284	Junos OS: MX240, MX480, MX960 platforms using MPC10E: Memory leak will be observed when subscribed to a specific subscription on Junos Telemetry Interface (CVE-2024-39518) Product-Group=junos Severity=Major	A Heap-based Buffer Overflow vulnerability in the telemetry sensor process (sensord) of Juniper Networks Junos OS on MX240, MX480, MX960 platforms using MPC10E causes a steady increase in memory utilization, ultimately leading to a Denial of Service (DoS). Please refer to https://supportportal.juniper.net/JSA82982 for more information.
PR Number	**Synopsis**	**Category: Key Management Daemon**
1771009	All the IPSec tunnels impacted due the kmd daemon crash when old dynamic security association_configuration is present Product-Group=junos	On Junos MX80, MX240, MX480, MX960 platforms with Multiservices Modular Interfaces Card (MS-MIC), Multiservices Modular Port Concentrators (MS-MPC) service cards, in an issue where an old dynamic security association_configuration (sa_cfg) for a tunnel is present and trying to establish

	Severity=Major	new sets of Internet Protocol Security Security Association (IPSec SAs) using a new Internet Key Exchange (IKE) SA established for the same remote device but with a different request. This can happen, if for some reason old sa_cfg is not cleaned (failed in clean-up). On crash, the Key Management Daemon (kmd) restarts but fails because of kernel instance mismatch present in the kernel database. So all the IPsec tunnels will be impacted.
PR Number	**Synopsis**	**Category: Layer 2 Control Module**
1763053	LLDP neighborship will not be formed on all Junos devices Product-Group=junos Severity=Major	On Junos and Junos OS Evolved platforms, LLDP (Link Layer Discovery protocol) neighborship will not come up on local device if the local device is using Junos version lower than 22.3 and remote device is using Junos version 21.4R3-S2 and its subsequent service releases or version higher than 22.3.
PR Number	**Synopsis**	**Category: Layer2 forwarding on EX/NTF/PTX/QFX**
1703412	Updated "show l2-learning vxlan-tunnel-end-point remote" now displays svtep for multiple routing instances Product-Group=junos Severity=Major	When configuration has evpn-vxlan, data vxlan configuration co-existence, show cmd updated to display svtep for both routing instance. "show l2-learning vxlan-tunnel-end-point source" "show interfaces vtep" command display Primary and Anycast IP address's of loopback interface.
1707878	Mac entry not ageout in RTG in EX4600-VC after VCP port reconnect Product-Group=junos Severity=Major	EX4600 with Redundant Trunk Group (RTG) configured, after VCP port between members of EX4600 disconnect and connect again. Mac address entry created in RTG cannot ageout.
1724489	Help string "Display information for a specified VLAN" is changed to "Display information for a specified bridge domain" Product-Group=junos Severity=Major	On Junos MX platforms, the help string for CLI command "show mac-vrf forwarding flood ?" vlan-name is changed from "Display information for a specified VLAN" to "Display information for a specified bridge domain"
1743737	The switch-options settings on the logical-system will be not reflected after RE rebooting or RE switchover or restart of l2-learning Product-Group=junos Severity=Major	The switch-options settings on logical-system will be not reflected after RE (Routing Engine) rebooting or RE switchover or l2-learning. This issue is seen only with logical-system and with the default instance, this behavior is not seen.
1757692	The ksyncd and vmcore core will be seen on backup RE when GRES is configured Product-Group=junos Severity=Major	This issue is seen on all Junos platforms when MAC-limit/storm-control feature is configured with action shutdown, and after interface shutdown action has taken effect. When the customer issues "clear ethernet-switching recovery-timeout" or interface recovery timeout expires and recovery time is configured via "set interfaces unit family ethernet-switching recovery-timeout ". After the interface recovers, if the customer configures GRES, the ksyncd and vmcore core will be seen on backup RE.
1771691	In the EVPN-VXLAN scenario due to unsynchronized MAC-IP database traffic is getting dropped Product-Group=junos Severity=Minor	On all Junos and Junos OS Evolved platforms with Ethernet Virtual Private Network-Virtual Extensible Local Area Network (EVPN-VXLAN) configured, with any configuration change around EVPN-VXLAN Route Target (RTT)/Bridge Domain (BD)/ifl and link flap, MAC-IP is not getting synced to all nodes and Address Resolution Protocol (ARP) is not getting resolved, resulting in traffic drop.
1783346	Junos OS and Junos OS Evolved: Upon processing specific L2 traffic, rpd can hang in devices with EVPN/VXLAN configured (CVE-2024-39517) Product-Group=junos Severity=Major	An Improper Check for Unusual or Exceptional Conditions vulnerability in the Layer 2 Address Learning Daemon (l2ald) on Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated, adjacent attacker to cause Denial of Service (DoS). Please refer to https://supportportal.juniper.net/JSA79175 for more information.
1790064	The l2ald process will crash, with rapid configuration changes followed by rpd and l2ald restart process Product-Group=junos Severity=Major	On all Junos and Junos OS Evolved platforms with EVPN -VXLAN and high scaling configuration, rapid configuration changes followed by restart of rpd and l2ald will result in l2ald process crash and traffic drop will be observed.
PR Number	**Synopsis**	**Category: lacp protocol**

1773702	MC-LAG will not work as expected on all platforms Product-Group=junos Severity=Major	On all Junos and Junos OS Evolved platforms, due to mis-wiring or unexpected design in MC-LAG topology, when all the Multi-Chassis Link Aggregation (MC-LAG) nodes including Customer Edge (CE) devices are rebooted at once, MC-LAG will not work as expected.
1773827	The LAG with member interface enabled with 'force-up' can flap after switchover Product-Group=junos Severity=Major	On Junos and Junos Evolved QFX/EX platforms if the member link of an AE (Aggregation Ethernet) interface is configured with force-up, the LAG (Link Aggregation Group) can flap after switchover through GRES (Graceful Routing Engine Switchover) or during ISSU (In Service Software Upgrade). Traffic that goes through the LAG will be dropped when the interface flaps.
PR Number	**Synopsis**	**Category: Label Distribution Protocol**
1687834	After disable/enable MPLS, targeted LDP session is not getting established Product-Group=junos Severity=Major	In MPLS (Multi Protocol Label Switching) environment, for an established LDP (Label Distribution Protocol) over an RSVP (Resource Reservation Protocol) targeted session, when 'set protocols mpls disable' is configured and then removed, the targeted LDP session does not get re-established.
1706064	LDP sessions flap when router-id is changed Product-Group=junos Severity=Major	On all Junos and Junos Evolved platforms, When LDP (Label Distribution Protocol) dual transport is enabled, LDP IPv4 connection ID is changed from dual transport IPv4 ID to router-id when router-id changes.
PR Number	**Synopsis**	**Category: authd (AAA) library code**
1725143	The "show network-access address-assignment address-pool-manager status command" reports APM not connected when in fact it is connected Product-Group=junos Severity=Major	When the APM server does not send a system-id, the output of the 'show network-access address-assignment address-pool-manager status' command reports APM not connected. We changed the output for the command to clarify the APM status.
PR Number	**Synopsis**	**Category: Issues related to Junos licensing infrastructure**
1721757	Uncleared alarm observed when any capacity license is used and installed multiple times Product-Group=junos Severity=Major	On Junos EX and MX platforms, when any capacity license is used and installed multiple times, causes uncleared alarm.
1747720	Alarm LED is lit due to LICENSE_EXPIRED on Virtual Chassis Backup even with the valid license. Product-Group=junos Severity=Major	When you enable a licensed feature like BGP on Virtual Chassis (VC), Alarm LED is lit due to LICENSE_EXPIRED on VC backup even with the valid license.
1759618	License-service crash is seen on Junos OS Evolved platforms Product-Group=junos Severity=Major	On Junos OS Evolved platforms, when license with unknown feature ID/platform reserved feature ID is added via configuration set system license keys key and then if License-service is restarted or system is rebooted or software upgrade is done then license service crashes and crash files are seen. This is a non service impacting issue.
1766515	A warning message is seen while installing a license key with an unknown feature Product-Group=junos Severity=Major	On all Junos platforms, a warning message is seen when installing the license key where features don't support the product.
1771376	License missing on VC member after reboot Product-Group=junos Severity=Critical	License will be lost on VC (EX4300/QFX) in non-preprovisioned set-up if member 0 is rebooted.
1775463	The RE goes into amnesiac mode upon license check validation failure Product-Group=junos Severity=Major	On all Junos and Junos Evolved Platforms, the RE (Routing Engine) goes into amnesiac mode upon reboot if node locked license is configured via the "set system license keys key <>".
PR Number	**Synopsis**	**Category: PTX1000 platform**

1770739	Reboot on PTX1k with image 22.3x60 causes fpc to reboot with "Fatal ASIC initialization error, Offlining FPC" Error message Product-Group=junosvae Severity=Critical	Reboot on PTX1k with image 22.3x60 causes fpc to reboot with "Fatal ASIC initialization error, Offlining FPC" Error message times
PR Number	**Synopsis**	**Category: Port-based link layer security services and protocols that a**
1710867	Traffic drop happens on IFLs which has MACsec configured Product-Group=junos Severity=Major	On MX2008/MX2010/MX2020 platforms with MPC11E, traffic drops are seen when MACsec(Media Access Control Security) is enabled on multiple (at least 2) IFLs (logical interface) on the same IFD (physical interface).
PR Number	**Synopsis**	**Category: SW PRs for MPC10E Interfaces**
1719682	LACP interface will be down after aggressive link flaps with 100ms interval Product-Group=junos Severity=Major	When link flaps repeatedly within a very short time frame on 100G interface on MPC10E line card supported platforms(MX240, MX480, MX960, MX2010, MX2020), traffic stops egressing the affected interface and report syslog messages during link down event. When there are continous flaps and if those flaps are very fast under 1 second and continuous then this issue will be seen.
1745317	MPC10E - PIC bounce/config change on a PIC with 10G QSA adaptor can cause a FPC restart Product-Group=junos Severity=Major	On MPC10E, if the PIC bounce (offline/online) or a config change is triggered with a PIC that has a QSA adaptor plugged in, the entire FPC can restart because of a core. The issue is only applicable to MPC10E platform. PIC bounce can cause the PFEMAN to hang, resulting in a fabric blackhole. This eventually will cause the entire FPC to restart because of the cmerror action.
PR Number	**Synopsis**	**Category: MPC11 ULC fabric software related issues.**
1753374	MPC11E suddenly goes offline due to power failure causing multitude fabric stream drain failures on all other MPC11 Product-Group=junos Severity=Major	If you have 2 or more MPC11 cards installed and a full mesh traffic flow and one MPC11 suddenly goes offline due to power failure, the other MPC11E cards might report fabric drain failure and a reboot of the line cards is needed to recover.
1766674	Traffic blackholed due to hardware errors like FPC/SIB power fail or Fabric Link errors Product-Group=junos Severity=Major	On Junos MX platforms with MPC11E, LC9600 line cards, traffic is blackholed due to hardware errors.
PR Number	**Synopsis**	**Category: MPC11 ULC interface software related issues.**
1698135	XQSS_CMERROR_DSTAT_INT_REG_DROP0_QDEPTH_UNDRN alarm is seen on MX2K platforms with MPC11E line cards upon aggregate interface down/flap event Product-Group=junos Severity=Major	On MX2010 or MX2020 platforms with MPC11E line cards, if a member link of an aggregate interface goes down or flaps, it might trigger "XQSS_CMERROR_DSTAT_INT_REG_DROP0_QDEPTH_UNDRN" alarm and disable-pfe action is executed. The affected PFE (Packet Forwarding Engine) will be disabled and no traffic will pass through it.
PR Number	**Synopsis**	**Category: Multiprotocol Label Switching**
1694957	The rpd process crash is seen when PCCD is deactivated Product-Group=junos Severity=Major	On all Junos and Junos Evolved platforms, deactivating PCCD (Path Computation Client Process) from MPLS (Multiprotocol Label Switching) Container LSP (Label Switched Path) might result in the rpd core. When the container LSPs are removed from the tag external controller, the cleanup of the members does not happen which results in the core.
1738774	Traffic blackhole due to an additional label when CCNH is toggled Product-Group=junos Severity=Critical	On all Junos and Junos Evolved platforms, with scaled Border Gateway Protocol (BGP) routes, when Chained Composite Next Hops (CCNH) is toggled, a few next-hops end up creating additional labels causing a traffic blackhole.
1773796	The LSP name and bandwidth values are displayed continuously in "show mpls lsp autobandwidth name X" command	In "show mpls lsp autobandwidth name X" command when the name of the Link State Packet (LSP) is greater than 21 characters, the first column with LSP name and the second column with the Last bandwidth are merged.

	Product-Group=junos Severity=Major	
PR Number	**Synopsis**	**Category: Multi Protocol Label Switch OAM**
1670711	VCCV BFD session will be down as the periodic ping will not work as expected in a seamless MPLS scenario Product-Group=junos Severity=Major	On all Junos and Junos Evolved platforms, the VCCV BFD (virtual circuit connection verification bidirectional forwarding detection) will not work in an MPLS (Multi-Protocol Labeled Switching) BGP-LU (Labeled Unicast) environment. This happens when a user configures VCCV BFD with PEs belonging to different network segments and the interface address of one PE is not learned by another PE. Due to this periodic ping will get failed and leads to some traffic loss.
PR Number	**Synopsis**	**Category: Multicast Routing**
1769782	The rpd crash is observed when mvpn-mode is configured as "rpt-spt" and multicast snooping is enabled Product-Group=junos Severity=Major	On Junos OS Evolved platforms, when mvpn-mode (Multicast Virtual Private Network) is configured as "rpt-spt" (Rendezvous-point tree - Shortest-path tree) and multicast snooping is enabled, the rpd crash is observed. The issue happens when the routing process tries to obtain the source address on processing the multicast <*, g> route.
1777774	The rpd process crash is observed when MVPN PE receives PIM join messages from the remote peers Product-Group=junos Severity=Major	On all Junos Evolved platforms, when MVPN (Multicast Virtual Private Network) configured device receives PIM join or IGMP report from the remote peer installs route in next-hop and not in multicast composite next-hop, causing the rpd process to crash.
PR Number	**Synopsis**	**Category: For multicast snooping on MX**
1711153	A crash can be observed for 'mcsnoopd' process when the VLAN name for igmp-snooping has certain characters Product-Group=junos Severity=Major	On all Junos and Junos Evolved platforms, a crash can be observed for the 'mcsnoopd' process. This issue is seen when the devices support the VLAN (Virtual Local Area Network) style of igmp-snooping (internet group messaging protocol configuration (set protocols igmp-snooping vlan) and the VLAN name begins with the word all and has certain other characters. The workaround is not to enable the snooping for such VLANs.
PR Number	**Synopsis**	**Category: Multicast for L3VPNs**
1709175	MVPN sender site not working with IR tunnels configured Product-Group=junos Severity=Major	On all Junos and Junos Evolved platforms, MVPN (Multicast Virtual Private Network) sender site having IR (Ingress Replication) tunnel configured, due to software issue, type 1 route is not being sent and egress node is observed to not accept traffic from unknown neighbor.
PR Number	**Synopsis**	**Category: MX Timing software**
1704606	A transit PTP packet is modified when passing through an MPC5E and MPC6G line card 100G ports part of PTP boundary/ordinary clock configuration Product-Group=junos Severity=Major	On Junos MX240/MX480/MX960/MX2020/MX2008/MX2020 platforms with MPC5E/MPC6E line-cards at 100G ports, Precision Time Protocol over IPv4/6 (PTPoIPv4/6) and Precision Time Protocol over Ethernet (PTPoE) encapsulations are enabled by default when "phy-timestamping" is configured. Since both of these encapsulation types are enabled on the interface, the transit PTPoIPv4/6 packets passthrough to the through PTP configured interfaces get interpreted and timestamped incorrectly, leading to clock drift at the end of the PTPoIPv4/6 consumer side. In an ideal situation, the transit PTPoIPv4/6 packets should be sent forth as normal packets without being altered.
1740709	SyncE FSM moves to unexpected state during clock selection Product-Group=junos Severity=Major	On Junos MX240/480/960/2010 platforms, a restart of non-PTP/Non-SyncE FPC while the SyncE clock selection is in progress, SyncE or PTP may be affected during this scenario.
1746984	PTP master feature will not work as expected Product-Group=junos Severity=Major	On MX240/MX480/MX960 platforms with SCBE3 (Enhanced Switch Control Board), PTP (Precision Time Protocol) master feature shall not work as expected. The qualified PTP CLK (8k) from RE (Routing Engine) will not propagate to other Line cards that are acting as Master to downstream nodes.
1750316	SyncE stuck in holdover upon PTP slot switchover	SyncE stuck in holdover upon PTP slot switchover without change in PTP phase

	without change in PTP phase align state Product-Group=junos Severity=Critical	align state.
1750885	MPC10E: Support of G.8275.1 PTP Hybrid mode with speed 25G and 400G Product-Group=junos Severity=Major	In 21.2R3S6 release, MPC10E line-card does not support of G.8275.1 PTP Hybrid mode with speed 25G and 400G
1752550	Unexpected behavior will be observed while PTP configured Product-Group=junos Severity=Major	When an existing PTP configuration is updated to use G.8275.1.enh and PTPoIPv4, on Aggregate Ethernet interfaces with member links across multiple line cards, may be out of sync on different line cards. The following alarm can be seen - "Simultaneously PTPoE & PTPoIP master/stateful streams not allowed on same line-card" - even when PTPoE and PTPoIPV4 on different line card.
1755479	CLI output is not correct during SyncE down PTP intact scenario Product-Group=junos Severity=Major	On MX240/MX480/MX960 platforms, the CLI output is incorrect when SyncE is down and PTP is intact.
1765772	FPC crash will be observed when issuing PIC offline/online commands Product-Group=junos Severity=Major	On MX240/MX480/MX960/MX2010/MX2020 platforms with MPC7, 8, 9, 10E, when issuing Physical Interface Cards (PICs) offline/online commands, Flexible PIC Concentrators (FPC) cores will be observed that causes FPCs to be restarted.
PR Number	**Synopsis**	**Category: Track Mt Rainier RE NIC issues in Linux**
1695794	The RE mastership switchover will not be triggered when the internal master interface on VMHost is down Product-Group=junos Severity=Major	On Junos Dual-RE VMHost platforms, the Flexible PIC Concentrator (FPC) will be disconnected and the Routing Engine (RE) mastership will not be triggered when the master internal interface(eth1/eth2) is down. Traffic loss will be seen as FPCs are disconnected.
PR Number	**Synopsis**	**Category: Odin Timing software**
1745604	[TWM Clocking Solution] - chassis clock status should not move to "holdover" while switching between PTP path alone Product-Group=junos Severity=Major	[TWM Clocking Solution] - chassis clock status should not move to "holdover" while switching between PTP path alone
PR Number	**Synopsis**	**Category: OS IPv4/ARP/ICMPv4**
1722708	ksyncd core with dhcp subscribers Product-Group=junos Severity=Major	On all Junos platforms, in a very rare scenario, when subscriber-management and NSR is enabled, there could be a temporary transition state where one subscriber prefix has 2 nexthop referred. In that state if a deletion happened for that particular prefix, the nexthop deletion is successfully done one master RE but the deletion is failed on the backup RE. This eventually causes nh index inconsistency and then ksyncd core on backup RE. The fix is to make sure the deletion on the backup can be done successfully.
1740873	ARP resolution will not work properly if the L3 interfaces are configured with native vlan-id Product-Group=junos Severity=Major	On MX platforms with MPC10/MPC11/LC9600 linecards and MX304, in problematic scenario if a device interface is configured with native vlan the packet goes out tagged and peer device receives tagged packet. If the peer device is not configured to expect tagged packets (either due to different native VLAN configuration or no VLAN configuration), the peer will drop the packet. Due to this, ARP (Address Resolution Protocol) resolution would fail which leads to traffic drop. Ideally if the L3 interfaces are configured with native-vlan id, the packets should go out untagged.
1752151	The ksyncd process crashes with replication error after performing restart routing Product-Group=junos Severity=Major	On Junos platforms with dual RE (Routing Engine), VRRP (Virtual Router Redundancy Protocol) configuration, GRES (Graceful Routing Engine Switchover) and NSR (Non-Stop Routing) enabled, ksyncd (Kernel Synchronization Daemon) process will crash post performing routing restart or rebooting master RE. This ksyncd process crash happens due to replication error on backup RE and will recover on its own. There will be no service impact on master RE.

1763706	Routing Protocol session down with native VLAN configuration on MX platforms Product-Group=junos Severity=Major	On certain Junos MX platforms, the IS-IS (Intermediate System to Intermediate System) sessions will not come up/keep flapping when the native VLAN (Virtual Local Area Network) is configured on the associated l3 interface. There will be traffic loss due to the routing protocols being down and the workaround for the issue is to remove the native VLAN configuration.
PR Number	**Synopsis**	**Category: FreeBSD Kernel Infrastructure**
1691036	NTP time drift Product-Group=junos Severity=Major	NTP time drift on the affected Junos releases. Earlier implementation of kvmclock with vDSO (virtual Dynamic Shared Object) which helps avoid the system call overhead for user space applications had problem of time drift, the latest set of changes takes care of initializing the clock after all auxiliary processors are launched so that the clock initialization is accurate.
PR Number	**Synopsis**	**Category: "ifstate" infrastructure**
1767098	Prolonged SNMP polling leads to kernel crash in SCU/DCU scenario Product-Group=junos Severity=Major	On all Junos platforms with SCU (Source Class Usage)/DCU (Destination Class Usage), SNMP (Simple Network Management Protocol) polling continuously for a longer duration will crash the kernel and affect network traffic.
PR Number	**Synopsis**	**Category: Kernel MPLS / Tag / P2MP Infrastructure**
1747365	rpd crash observed during RE switchover or Route Convergence Product-Group=junos Severity=Major	On Junos EX and QFX platforms, where in few cases during an RE (Routing Engine) switchover (caused by rpd crash on the master RE), rpd (routing protocol daemon) crash is observed on the backup RE once it becomes the master. This results in complete network outage.
PR Number	**Synopsis**	**Category: IPv6/ND/ICMPv6 issues**
1704114	The next-hop is shown as unicast instead of reject even when the IPv6 neighbor is unreachable Product-Group=junos Severity=Major	When a neighbor route is unreachable, the IPv6 neighbor state should have been changed back to HOLD, instead, it stays as unicast. This causes impact in the forwarding plane traffic.
PR Number	**Synopsis**	**Category: JUNOS Network App Infrastructure (for ping, traceroute, etc)**
1717843	JUNOS - FILE COPY - Secure file copy using VRF succeeds even on disabling VRF Product-Group=junos Severity=Critical	JUNOS - FILE COPY - Secure file copy using VRF succeeds even on disabling VRF
1746779	show system connections show-routing-instances; reports all routing-instances as unknown. Product-Group=junos Severity=Major	Show system connections show-routing-instances; reports all routing-instances as unknown.
PR Number	**Synopsis**	**Category: PFE Peer Infra**
1747077	Due to timing issues, PFE/PICs will be slow and traffic will be impacted on all Junos platforms Product-Group=junos Severity=Major	On all Junos platforms, due to timing issues the PFE (Packet Forwarding Engine) /PICs (Physical Interface Card) will be slow and services will face slowness issue and error message: 'Minor potential slow peers are: X' will be seen. This is rare timing issue.
PR Number	**Synopsis**	**Category: TCP/UDP transport layer**
1700438	The TCP sessions for BGP are closed on the backup RE Product-Group=junos Severity=Major	On all Junos Platforms, if the interface configuration is altered to switch from one routing instance to another it might result in the closing of BGP session on the Backup Routing Engine.
1761242	TCP window scaling may be not applied to the first TCP	On all JUNOS platforms, the first TCP packet sent by Junos to the client after

	packet sent to the client after the three-way handshake, leading to unnecessary segmentation. Product-Group=junos Severity=Major	the three-way handshake may be unnecessarily segmented due to TCP window scaling option being not applied even if it was negotiated.
PR Number	**Synopsis**	**Category: Kernel Tunnel Interface Infrastructure**
1712352	Master and Backup RE synchronization issue will be seen if chassisd is restarted on Master RE Product-Group=junos Severity=Major	On all Junos platforms with GRES (Graceful Routing Engine Switchover) and NSR (Non Stop Routing) enabled, Master and Backup RE (Routing-Engine) synchronization issues will be seen when chassisd (Chassis process) is restarted on Master RE. The ksyncd (Kernel Synchronization) process crash will be observed on the backup RE. If failover happens post this event, traffic would be impacted. This is a rare issue.
1743306	FTI interface status (up/down) does not sync between master and backup RE. Product-Group=junos Severity=Critical	FTI IFD's and IFL's are not cleaned up on new backup in a switchover where graceful-switchover is not configured. This leads to mismatch between interface status or even commit error.However, with gres config "set chassis redundancy graceful-switchover", no issue is seen.
PR Number	**Synopsis**	**Category: OSPF routing protocol**
1702456	Junos prefers SRMS advertised label over IS-IS/OSPF SID label advertised via opaque-AS Extended-Prefix Product-Group=junos Severity=Major	On all Junos and Junos Evolved platforms, when IPv4 prefix advertisement received by an IS-IS/OSPF router in the Extended IP reachability TLV and SR mapping server (SRMS) advertisement for the same prefix received through the segment identifier (SID) label Binding TLV, then SRMS advertised label preferred over IS-IS/OSPF SID label advertised via opaque-AS Extended-Prefix. Traffic will be sent via wrong path due to this issue.
1704521	On all Junos and Junos OS Evolved platforms, the TI-LFA and Legacy LFA are mutually exclusive, and the commit check will fail and blocks LFA on one instance Product-Group=junos Severity=Major	On all Junos and Junos OS Evolved platforms, if configuring LFA (Loop-Free Alternate)/RLFA (Remote LFA)/PPLFA (Per-prefix LFA) in the routing-instance and TI-LFA (topology independent LFA) in the master instance, along with Segment Routing and node-link-protection with post-convergence, the commit check fails and blocks LFA on one instance.
1732500	The adjacent PE Node SID label will drop from routing table when MicroLoop-Avoidance is enabled in OSPF-SR Product-Group=junos Severity=Major	On all Junos and Junos OS Evolved platforms when OSPF MicroLoop-Avoidance(MLA) is enabled on Segment Routing(SR) speaking node connected to LDP speaking node and this same SR node has to do SR-LDP stitching, the LDP route on the LDP facing interface will be withdrawn and eventually withdraws the node SID label if there has either LDP speaking node facing link flapping or the rpd is restarted.
1737978	OSPFv3 using the VIP address on the IRB interface will not form adjacencies between peers Product-Group=junos Severity=Major	OSPFv3 may not form adjacencies on IRB interfaces with VRRP configuration.
PR Number	**Synopsis**	**Category: PFE COS features on PE based platforms**
1725833	Traffic drop and error message observed during boot time on certain QFX platforms Product-Group=junos Severity=Major	On Junos QFX10002, QFX10008, QFX10016 platforms, it is observed that that during upgrade when device is booted, the error message " dc-t10qfx10002-4-q fpc0 PFE_ERROR_FAIL_OPERATION: IFD:xe-0/0/22:3 chip0: is_pvq:0 vpfe12 state lookup failed forpvq_offset:0 vpfe12=17" is observed and there is traffic drop.
PR Number	**Synopsis**	**Category: Express Chip L3 software**
1621976	BFD session flap might be observed in scaled scenario Product-Group=junos Severity=Major	On Junos QFX10k platforms with scaled number of BFD (Bidirectional Forwarding Detection) sessions configured, addition of a new BFD session might cause flapping in newly added session and other existing BFD sessions.
1740190	Page allocation and next-hop installation failures on Junos PTX and QFX Product-Group=junos Severity=Major	On certain PTX and QFX platforms, when unicast/multicast and Point-to-multipoint communication (P2MP) next-hops are present at a high scale, which leads to page allocation failures to f-label page allocation and next-hop installation failures, eventually leading to traffic loss.

1756672	Learning stops in logical interface in QFX10K platforms Product-Group=junos Severity=Major	On Junos QFX10K platforms from 21.2 release, when there are more than four SP style logical interface configured with same vlan or with vlan-id-list, then issue is seen in logical interfaces.
1761579	The FPC will crash on Junos PTX platforms in a rare timing issue Product-Group=junos Severity=Major	On Junos PTX platforms with with FPC3, JNP10K-LC1101, JNP10K-LC1102, JNP10K-LC1104, JNP10K-LC1105 and PTX10000, during a rare race condition in hostbound packet handler thread, the FPC (Flexible PIC Concentrator) might crash leading to all the interfaces going down. The exact trigger for this issue is unknown.
1761887	ECMP traffic drop after the AE interface flap Product-Group=junos Severity=Major	On Junos OS PTX and QFX platforms, in a race condition after the AE (Aggregated Ethernet) interface flap, PFE (Packet Forwarding Engine) will not update unilist next-hops with flapped AE next-hop correctly, causing ECMP (Equal-Cost Multi-Path) traffic drop.
PR Number	**Synopsis**	**Category: Express Paradise PFE Sflow**
1741461	Enabling sflow triggers ddos-protection violation of protocol group resolve Product-Group=junos Severity=Major	On all Junos based QFX platforms, when sflow is enabled with ECMP, ddos-protection violation of protocol group resolve is triggered. Sampled packets will be dropped and sflow will stop sending packets to the collector. This is a non-service impacting issue, however sflow will be impacted.
PR Number	**Synopsis**	**Category: vpls on branch (jseries and srx) platforms**
1712161	SRX3xx series may stop responding to SNMP requests when a wireless mPIM is installed. Product-Group=junos Severity=Major	SRX3xx series may stop responding to SNMP requests when a wireless mPIM is installed. The wireless card times out responses to system SNMP requests which may then lock up SNMPD. There is no workaround, but recovery is to restart snmpd.
PR Number	**Synopsis**	**Category: Phone-Home-Client Infrastructure**
1743222	After ZTP process, the configuration fetch from the script path in event-options is impacted Product-Group=junos Severity=Major	On EX4300-MP platforms, when event-options are configured and ZTP (Zero Touch Provisioning) is performed, the configurations are not retrieved as the script path is not configured properly.
PR Number	**Synopsis**	**Category: Protocol Independant Multicast**
1709038	Junos OS and Junos OS Evolved: Receipt of specific PIM packet causes rpd crash when PIM is configured along with MoFRR (CVE-2024-39558) Product-Group=junos Severity=Major	An Unchecked Return Value vulnerability in the Routing Protocol Daemon (rpd) on Juniper Networks Junos OS and Juniper Networks Junos OS Evolved allows a logically adjacent, unauthenticated attacker sending specific PIM packet to cause rpd to crash and restart, resulting in a Denial of Service (DoS), when PIM is configured with Multicast-only Fast Reroute (MoFRR). Continued receipt and processing of this packet may create a sustained Denial of Service (DoS) condition. Please refer to https://supportportal.juniper.net/JSA83018 for more information.
PR Number	**Synopsis**	**Category: Issues related to PKI daemon**
1694604	IPSEC tunnel is not getting established back after the execution of 'clear security ike sa' Product-Group=junos Severity=Major	On Junos SRX platforms, the IPSEC (Internet Protocol Security) tunnels do not get established after the tunnels are deleted using the command 'clear security ike sa'.
1745288	Junos OS: An invalid certificate causes a Denial of Service in the Internet Key Exchange (IKE) process (CVE-2024-30397) Product-Group=junos Severity=Major	An Improper Check for Unusual or Exceptional Conditions vulnerability in the the Public Key Infrastructure daemon (pkid) of Juniper Networks Junos OS allows an unauthenticated networked attacker to cause Denial of Service (DoS). Please refer to https://supportportal.juniper.net/JSA79179 for more information.
PR Number	**Synopsis**	**Category: PTX10K Routing Engine**
1698894	The communication between primary and backup	On PTX Series routers and QFX Series switches with dual Routing Engines running

	Routing Engines breaks in the event of scale network churn Product-Group=junos Severity=Major	Junos OS, high host-bound traffic can cause a memory issue. Because of low memory, the Address Resolution Protocol (ARP) entry add can fail. Due to this, the communication between the primary Routing Engine and backup Routing Engine breaks, causing redundancy failure in high network churn and GRES-enabled scenario.
PR Number	**Synopsis**	**Category: QFX access control list**
1750828	The PFE process crashed while removing and applying the firewall filters Product-Group=junos Severity=Major	On Junos QFX5K/EX (except EX4300) platforms, the Packet Forwarding Engine (PFE) crash is observed while applying the firewall filters.
1754929	[QFX5120]Egress filter does not work properly on vlan pop configuration Product-Group=junos Severity=Major	On QFX5120 platform if it sets egress filter on vlan pop configuration, filter does not work properly
PR Number	**Synopsis**	**Category: QFX PFE Class of Services**
1688455	The FPC crash would be observed when the same CoS configuration is applied with wildcard for all the physical interfaces and AE Product-Group=junos Severity=Major	On all Junos platforms, in a scaled scenario when some of the ge/xe/et interfaces are members of Aggregated Ethernet (AE) and the Class of Service (CoS) forwarding-class-set configuration is applied with a wildcard for all the physical interfaces and AE, it would trigger a Flexible PIC Concentrators (FPC) crash which leads to traffic loss.
1761884	Junos OS: QFX5000 Series and EX4600 Series: Output firewall filter is not applied if certain match criteria are used (CVE-2024-39533) Product-Group=junos Severity=Major	An Unimplemented or Unsupported Feature in the UI vulnerability in Juniper Networks Junos OS on QFX5000 Series and EX4600 Series allows an unauthenticated, network-based attacker to cause a minor integrity impact to downstream networks. Please refer to https://supportportal.juniper.net/JSA82993 for more information.
PR Number	**Synopsis**	**Category: DHCP related Issues**
1711525	DHCPv6 packets could not be forwarded if it contains the trailer or extra bytes out of the IP stack Product-Group=junos Severity=Major	On all Junos QFX5K and EX platforms with DHCPv6 (Dynamic Host Configuration Protocol) relay configuration, IPV6 (Internet Protocol) assignment could not take place as the DHCPv6 solicit packets containing extra bytes in DHCPv6 header trailer are not getting forwarded to the DHCP server.
PR Number	**Synopsis**	**Category: QFX L2 PFE**
1718095	Deleting the MAC-VRF routing instance will lead to a traffic drop for other routing instances Product-Group=junos Severity=Major	On Junos QFX5K and EX platforms configured with EVPN-VXLAN (Ethernet Virtual Private Network-Virtual Extensible LAN), deleting instance-type MAC-VRF for a routing instance will lead to the traffic drop for the other MAC-VRF routing instances as well.
1736348	BFD session remains stuck in INIT state on certain QFX and EX platforms Product-Group=junos Severity=Major	On Junos QFX5120-48Y/EX4650-48Y/QFX5120-32C platforms, when the MAC (Media Access control) address corresponding to a next hop is updated, the BFD (Bidirectional Forwarding Detection) endpoints that are using this Next hop/egress is not picking up the updated MAC address and as result BFD session remains in INIT state and causes traffic impact.
1739048	Q-in-Q for access port to access port through VxLAN bridge-domain does not work on all Junos QFX5K platforms Product-Group=junos Severity=Major	Q-in-Q for access port to access port is not working on all Junos QFX5K platforms when it is configured with VxLAN local switching (bridge-domain). The traffic is working in only one direction and the packet is getting dropped in reverse direction because the packet is coming in as single tagged VLAN.
1759875	The unexpected file is generated on Junos QFX/EX platforms when executing RSI command Product-Group=junos Severity=Minor	After executing "request support infomation | save " command, unexpected file will be generated.
1763116	VPLAG information not installed correctly in hardware results in traffic flooding	On QFX5k and EX4100, EX4300, EX4400, and EX4650 platforms in the EVPN-VXLAN environment, when the underlay links flaps are observed followed by IPC

	Product-Group=junos Severity=Major	(Interprocess communication) out-of-order events lead to VPLAG (Virtual Port Link Aggregation) information not correctly installed in hardware resulting in traffic flooding.
1771183	Memory leak observed on non-local FPC for Junos QFX5K and EX platforms Product-Group=junos Severity=Major	On Junos QFX5K and EX platforms in virtual chassis (VC), memory leak happens for non-local Flexible PIC Concentrators (FPC) when delete/detach of interface is performed.
1781955	A few AE interfaces will drop traffic when a large number of AE interfaces are deleted and added back Product-Group=junos Severity=Major	On EX4100, EX4100 Multigigabit, EX4100-F, EX4400, EX4400 Multigigabit, EX4650-48Y, QFX5120-48Y, QFX5120-32C, QFX5120-48T, QFX5110 and QFX5120-48YM platforms with Ethernet VPN-Virtual Extensible LAN (EVPN-VxLAN) configured, a few AE interfaces will drop traffic when a large number of Aggregated Ethernet (AE) interfaces are deleted and added back. When this issue happens AE interfaces will be UP but traffic would be dropped.
PR Number	**Synopsis**	**Category: QFX L3 data-plane/forwarding**
1666260	Traffic is not restored when l2circuit configurations are deleted and added back on QFX5K Product-Group=junosvae Severity=Major	On the QFX5000 line of switches running Junos OS, when flapping the Layer 2 circuit (access) ports or removing and re-adding the l2 circuit configuration, the programming of the access side port fails and traffic ingressing or egressing out of it gets dropped.
1700927	Minor packet drops due to hardware programming issues Product-Group=junos Severity=Major	On QFX5110-32Q platform, due to hardware programming issues minor packet drops (0.01%) will be observed for the traffic over the VC (Virtual Chassis) interface.
1742763	Traffic drop will be observed after extended-vni-list configuration change with EVPN-VXLAN scenario Product-Group=junos Severity=Major	On Junos QFX5100/QFX5110/QFX5120/QFX5200/QFX5210/EX4100/EX4300-MP/EX4400-XX platforms having Ethernet VPN-Virtual Extensible LAN (EVPN-VXLAN) configured if extended-vni-list configuration is deleted, the network interface is flapped and when extended-vni-list is added back due to this traffic using the Flood NH (BUM) on the device will be lost.
1748462	Unable to install IPv6 routes in LPM table Product-Group=junos Severity=Major	On Junos platforms QFX5200 and QFX5210 with custom-profile set under "set chassis forwarding-options", traffic for routes IPv4/IPv6 would be impacted due to hardware limitation.
1763667	BFD session detection time is higher than expected leading to traffic drop Product-Group=junos Severity=Major	On QFX5K and EX4K platforms, when using HW (Hardware) assisted inline BFD (Bidirectional Forwarding Detection), the detection timer for the sessions is higher than what is configured. Hence, the BFD packets mirrored to the CPU get dropped at the host path.
1767190	An unnecessary traffic load on the peer boxes Product-Group=junos Severity=Major	L3 Multicast with TTL=1 get forwarded.
1771630	Family ethernet-switching policer per-sub-unit interface breaks after dcpfe/device restarts Product-Group=junos Severity=Major	On all Junos QFX and EX platforms, on dcpfe/device reboot, the firewall filters will not be processed affecting the filters applied on subunits of the LAG interfaces.
1782762	MTU Adjustment on Junos QFX5K platforms with GRE Causes FPC and Link Partner FPC Reboots Product-Group=junos Severity=Major	On Junos QFX platforms with Generic Routing Encapsulation (GRE) tunnels enabled, when attempting to adjust the MTU (Maximum Transmission Unit) configuration of a physical interface, a reboot of the FPC is triggered which would leads to crash and impacts the traffic.
PR Number	**Synopsis**	**Category: qfx-sw-mclag**
1742613	Race condition where FLOOD ROUTE DEL event can cause l2ald crash. Product-Group=junos Severity=Major	When system comes up with BULK L2 config, a subsequent CONFIG delete in a way that L2ALD is still not finished processing the config create, could lead to a race condition where FLOOD ROUTE DEL event can cause l2ald crash.
PR Number	**Synopsis**	**Category: QFX MPLS PFE**
1731291	Traffic for VLAN-id 2 gets dropped in Ethernet-CCC L2	On Junos QFX5k and EX4650 platforms traffic drop for VLAN (Virtual Local Area

	Circuit on QFX5k/EX4650 platforms Product-Group=junos Severity=Major	Network) having id 2 will be seen in the Ethernet-CCC (Circuit Cross Connect) L2 circuit. This happens because the VLAN-id is getting stripped at the egress PE (Provider Edge Router) hence causing a traffic drop at the CE (Customer Edge) Router.
1742364	Traffic dropped is observed in the MPLS LDP scenario when the peer device MAC address is changing Product-Group=junos Severity=Major	On Junos QFX5100 and EX4600 platforms when there is MAC (Media Access Control) change for the LDP (Label Distribution Protocol) neighbor and IP remains the same, the ARP (Address Resolution Protocol) update is proper but MPLS LDP may still use the stale MAC address of the neighbor. If there is any application/service such as MP-BGP using LDP as next-hop, all transit traffic pointing to the stale MAC address will be dropped.
PR Number	**Synopsis**	**Category: QFX analyzer, sflow**
1777265	The fxpc process crash is seen on a specific Junos QFX and EX platforms except EX4300 due to memory leak after VTEP IFLs configuration and un-configuration Product-Group=junos Severity=Major	VTEP (VXLAN Tunnel Endpoint) IFLs (Logical Interfaces) configuration and un-configuration causes a memory leaks and it leads to the fxpx process crash on a specific Junos QFX and EX platforms except EX4300.
PR Number	**Synopsis**	**Category: QFX EVPN / VxLAN**
1718485	Overlay ARP entries will not resolve or be delayed on Junos QFX5k and EX platforms Product-Group=junos Severity=Minor	On Junos QFX5K and EX4K Platforms configured with VxLAN, the overlay ARP packet from the access side is sent to CPU Q-7 which is the VxLAN queue & from VTEP is sent to CPU Q-5 which is the Overlay-ARP queue. This change is implemented starting from the following releases: 22.2R3-S3, 22.3R3-S2, 22.4R3, 23.1R2, 23.2R2, 23.3R1 and 23.4R1.
1721297	FPC crash on QFX5120-48Y Product-Group=junos Severity=Minor	If we observe any slowness in accessing the VTY and could see any hogging/scheduler slip messages in syslog. It is advised to run the debug commands manually, instead of running it via RSI.
1738276	High convergence time in the EVPN-VxLAN uplink failover scenario Product-Group=junos Severity=Major	On Junos QFX5K platforms in the EVPN-VxLAN scenario, due to high convergence time, traffic loss is more than expected when the uplink to the spine disabled (CLI initiated uplink failover).
1756407	Layer 2 VXLAN and Layer 3 IPv4 Logical Interfaces are not getting configured on the same interface Product-Group=junos Severity=Major	On Junos ACX/QFX/EX platforms, layer 2 Virtual Extensible LAN (VXLAN) and Layer 3 IPv4 logical Interfaces are not getting configured on the same interface.
1757364	The ARP entry is not completed without the l3-interface part of the VLAN with proxy-arp/arp-suppression Product-Group=junos Severity=Major	On QFX5110/QFX5120/QFX5200/QFX5210/EX4400/EX4100 platforms, the ARP entry will not be completed leading to traffic impact. The issue will be seen in EVPN-VXLAN (Ethernet VPN-Virtual Extensible LAN) scenario with storm-control and "arp-suppression"configured. The issue will only be seen when IRB was present and then it was deleted, if it is configured back, then the issue is not seen.
1760823	Traffic drop will be seen when packets are sent with incorrect VLAN tag Product-Group=junos Severity=Major	EVPN (Ethernet VPN) proxy arp with Multihome AE (ESI) responds with an incorrect VLAN (Virtual Local Area Network) tag. QFX5K, EX4400, and EX4650 platforms return proxy arp reply with incorrect vlan-id with native VLAN under ESI (Ethernet Segment Identifier) ae interface.
1771739	The PVST BPDU packet get dropped in transparent EVPN-VXLAN on the ingress PE-CE port of SP style on Junos EX/QFX platforms Product-Group=junos Severity=Major	On Junos QFX/EX platforms with SP (Service Provider)-style configuration and in the EVPN (Ethernet Virtual Private Network)-VXLAN (virtual Extensible Local Area Network) scenario at the ingress port of the CE (Customer Edge) host, PVST (Per VLAN Spanning Tree) VSTP (VLAN Spanning Tree Protocol) BPDUs (Bridge Packet Data Unit) are getting dropped when the VLAN-ID is set to none. It should be flooded into the VLAN (Virtual Local Area Network) including intra-VLAN ports and remote VTEP (Virtual Tunnel Endpoint).
1773676	The tagged traffic drop will be seen with vlan-id-list and native-vlan-id configured on one IFL. Product-Group=junos Severity=Major	On QFX5120, EX4650, and EX4400 platforms, when vlan-id-list and native-vlan-id are configured on one IFL, the packets will drop and will impact the tagged traffic.

1774366	The dcpfe process crash due to stale memory Product-Group=junos Severity=Major	On Junos QFX platforms, stale memory references are causing dcpfe crashes triggering PFE (Packet Forwarding Engine) to restart resulting in traffic disruptions.
1775672	The untagged packets get dropped in transparent EVPN-VXLAN on the ingress PE-CE port of SP style on certain Junos EX/QFX platforms Product-Group=junos Severity=Major	On Junos QFX5k/EX4650/4400/4100 platforms with SP (Service Provider)-style configuration and in the EVPN (Ethernet Virtual Private Network)-VXLAN (virtual Extensible Local Area Network) scenario at the ingress port of the CE (Customer Edge) host, untagged packets are getting dropped when native VLAN (Virtual Local Area Network) is configured. These packets should be flooded into the VLAN (Virtual Local Area Network) including intra-VLAN ports and remote VTEP (Virtual Tunnel Endpoint).
1781691	With EVPN-VXLAN configured, when a Layer 3 interface or underlay IRB interface deletion results in a traffic blackhole Product-Group=junos Severity=Major	On QFX5K and EX4K platforms in the EVPN-VXLAN (Ethernet Virtual Private Network - Virtual Extensible LAN) environment, a traffic blackhole is observed when we delete the L3 or underlay IRB (Integrated Routing and Bridging) interface, both the L3 egress and ingress hardware interface are deleted.
1783397	The fxpc process crash and the device reboots after deleting Aggregated Ethernet (AE) Interface along with its associated physical interface and then applying new interface configuration on the associated physical interface in an EVPN-VXLAN scenario Product-Group=junos Severity=Major	On an Ethernet Virtual Private Network (EVPN) / Virtual eXtensible Local-Area Network (VXLAN) scenario, after removing an Aggregated Ethernet (AE) Interface along with its associated physical interface on a QFX5k series device and then applying any configuration to the physical interface, the fxpc process crashes and the device undergoes an automatic reboot.
PR Number	**Synopsis**	**Category: QFX5100 Platfom related issues. CPLD, FPGA, FRU, Host, RE**
1727834	Configuration load failure from event script fails on QFX5100-48S-6Q after upgrading to 21.4R3 Product-Group=junos Severity=Major	On QFX5100-48S-6Q, the device configuration load via event script fails after performing an upgrade to the 21.4R3 release. This issue is encountered when the switch configuration includes an "event-options event-script file unconfigured-port-event.slax" and the slax file contains an embedded event policy. If the issue is encountered, log in via the console with the root user and delete the event-options event-script file unconfigured-port-event.slax (slax files) that contains an embedded policy.
PR Number	**Synopsis**	**Category: QFX5100 Virtual Chassis**
1746788	[QFX5K]When RSI(request support information) is executed in the VC configuration, some errors output Product-Group=junos Severity=Minor	On QFX5K platform, "request pfe execute ... target fpc" in RSI is always executed on master role in the VC configuration.
PR Number	**Synopsis**	**Category: QFX5200/5110/5120/5210 ISSU Infrastructure**
1713010	QSFP-100G-LR4-T2 optics will stay down after ISSU/TISSU Product-Group=junos Severity=Major	On all Junos Platforms that support optical transceiver QSFP-100G-LR4-T2 (740-061409), the transceiver remains down after an ISSU (In-Service Software Upgrade) or TISSU (Topology-Independent In-Service Software Upgrade) as the FEC (Forward Error Connection) mode gets enabled which is unsupported. The transceiver remains down and all the traffic passing through the optic will be impacted.
PR Number	**Synopsis**	**Category: QFX5200/5110/5120/5210 Platform optics related issues**
1698228	The physical interface link is not coming up after performing interfaces flapping on the QFX5120 device after starting traffic Product-Group=junos Severity=Major	On Junos QFX5120 platforms, when 100G physical interfaces are disabled and enabled, the physical interfaces will go down.
1726707	On QFX5120-48y-8c platform 10G ports go down in a port group if 25G SFP is inserted in the same group Product-Group=junos Severity=Major	QFX5120-48y-8c platform, if a 25G SFP is inserted in 10G speed configured port which is also a part of port group, all the interfaces in same port group will go down. Traffic will be impacted as all the interfaces in port group is going down.

1728452	[EX/QFX] debugging command "show aq107 xxx" on VTY may generate an error on 10GBASE-T SFP if AQ index exceeds 48. Product-Group=junos Severity=Minor	This is a debugging VTY command as you may be asked to issue the command by JTAC engineer during Trouble shooting. The "show aq107 xxx" command may generate an error on 10GBASE-T SFP
PR Number	**Synopsis**	**Category: QFX5200/5110/5120/5210 Platfom issues**
1709938	VC members are split when removing and inserting em0 cable Product-Group=junos Severity=Major	On QFX5120-48YM, QFX5120-48Y-8C, QFX5120-32C and EX4650-48Y platforms, when the management em0 cable is removed and reinserted in the Virtual Chassis (VC) environment, the VC members will split into separate VCs. The VC members will remain in the split state for approximately 5 mins.
1721313	Dcpfe core observed on upgrade from 22.4I to 22.4R2 on QFX5210-64C Product-Group=junosvae Severity=Critical	On the Junos QFX5210-64C platform, on upgrade from 22.4I to 22.4R2, due to PCIe address corruption during bootup time, dcpfe core is observed.
1729647	The fpc detaching logs will be seen when the VC port between different FPCs are flapped Product-Group=junos Severity=Major	When VC ports are flapped on QFX5100 and EX4600 devices, VC might get split and we might observe the logs which impacts the traffic flow.
1739808	QFX5120-48Y : The information of auto negotiation on SFP-T is not displayed Product-Group=junos Severity=Major	On QFX5120-48Y which is using SFP-T, the information of auto negotiation is not displayed.
1754838	The VC port stays down after backup becomes master Product-Group=junos Severity=Major	On QFX series platforms, virtual-chassis doesn't get formed when using 100G for VC port when unplug and plug 100G optics or DAC cable (Direct Attached Cable) which means converting VC port to network port and again to VC port via CLI command. This issue happens when a single Virtual Chassis Port (VCP) link between the master and backup breaks up, the backup will become the master again enable the VC port links, it won't come up. It will stay in master-master because VC port remains down.
1758868	100G optics set to CAUI4 on Junos QFX5200-32C platforms Product-Group=junos Severity=Minor	The Port interface is set wrong on 100G optics on QFX5200-32C platform.
1763499	Fan spinning upgraded alarm seen on QFX5110-32Q Product-Group=junosvae Severity=Major	On QFX5110-32Q fan speed upgraded alarm seen sometime for any fan tray fan 1 even if the fan is rotating normally, This has no functional impact.
1768554	Virtual chassis formation fails for VCP ports Product-Group=junosvae Severity=Major	On platforms that support QFX5E image and that support virtual chassis, when em0 is configured or em0 of master is plugged out, VC formation fails when network port is converted to vcp (Virtual Chassis port) port.
1779624	On the QFX5110-48S platform the virtual chassis port goes down when the VC is upgraded or the VC ports are deleted and added back Product-Group=junos Severity=Major	One of the virtual chassis ports in a VC of QFX5110-48S goes down either by deleting or adding the port or by upgrading the virtual chassis thereby causing a loss of redundancy for the virtual chassis ports. The ways to recover are by re-creating the VC or by doing soft removal and insertion of the port (please contact JTAC for the same).
PR Number	**Synopsis**	**Category: Issues related to dynamic-tunnels routing infrastructure**
1749601	Traffic is getting dropped when using GRE NH-based with GRE Key even though the dynamic tunnel is up Product-Group=junos Severity=Major	On all Junos and Junos OS Evolved platforms that support MPLS(Multi-Protocol Label Switching) over GRE (Generic Routing Encapsulation) and have dynamic tunnel configured the traffic can get dropped. This issue is seen when IPv4 traffic is sent and the NH (Next Hop) is a GRE-based dynamic tunnel with a GRE key, the traffic can get dropped even though the tunnel is in up state.
PR Number	**Synopsis**	**Category: RPD infrastructure issues related to NSR, GRES, switchover,**
1727957	The traffic drop is observed during the Graceful restart	On all Junos and Junos Evolved platforms, during the time of Graceful

	on Junos and Junos Evolved platforms Product-Group=junos Severity=Major	restart(GR), the routes in the Multiprotocol Label Switching(mpls).0 table will be updated even when the routing protocols are in the process of re-convergence and have not yet come out of GR. This causes inaccurate routes in the routing table and traffic drop is observed during GR.
PR Number	**Synopsis**	**Category: RPD Interfaces related issues**
1709629	RPD CPU utilization is 100% when configured with virtual router-advertisement for AE interface Product-Group=junos Severity=Major	On all Junos and Junos OS Evolved platforms rpd (Routing protocol daemon) CPU utilisation reaches 100% when configured with virtual router-advertisement for AE interface due to which AE member link flaps.
PR Number	**Synopsis**	**Category: KRT Queue issues within RPD**
1738820	An rpd crash will be observed due to inconsistency between rpd and kernel Product-Group=junos Severity=Critical	On Junos and Junos Evolved platforms, an rpd crash will be observed when rpd tries to add composite next-hop with the same parameters as in the kernel existing composite next-hop which is marked deleted but not deleted due to some reference.
1758483	The rpd memory leak using multicast composite nexthops Product-Group=junos Severity=Major	On Junos OS Evolved platforms, memory leak in the rpd (routing process daemon) will be observed when there is a change in the multicast composite nexthops (MCNH) via route changes. Please refer to https://supportportal.juniper.net/TSB74067 for more information.
1761667	The rpd process and chassisd process crash is seen Product-Group=junos Severity=Major	On Junos and Junos Evolved platforms configuring BGP causes the rpd to crash abnormally and later chassisd crashes too.
1774975	Features utilizing inactive routes will not work properly after the device reboot Product-Group=junos Severity=Major	On all Junos and Junos OS Evolved platforms, due to some software issue, after the device reboot features utilizing inactive routes in the routing table will not work properly. This will cause issues like some inactive routes not being advertised when selected as the best path, features like advertise-inactive not working properly as it utilizes an inactive route flash, high Routing Protocol Daemon (rpd) Central Processing Unit (CPU) utilization, etc.
PR Number	**Synopsis**	**Category: RPD Next-hop issues including indirect, CNH, and MCNH**
1747992	The memory consumption increases due to memory leak Product-Group=junos Severity=Major	On all Junos and Junos OS Evolved platforms, a continuous memory leak is observed due to an allocated socket memory not being freed. This is a minor leak but can lead to significant memory usage on highly scaled setups leading to performance and functional impact including system crash beyond a certain point.
1768604	Traffic blackhole due to incorrect NH entries with incorrect filter-id in CCNH table Product-Group=junos Severity=Major	On all Junos platforms, the firewall filter mapping in Routing protocol process(rpd) table goes out of sync with the Dynamic Firewall process(dfwd) and hold old filter-id value in filter entry which leads to incorrect next-hop(NH) entries in Chained composite next hops(CCNH).
PR Number	**Synopsis**	**Category: Shard routing infrastructure within RPD**
1727528	The rpd process can crash during a race condition when BGP rib-sharding is configured Product-Group=junos Severity=Major	On all Junos and Junos OS Evolved platforms, when BGP RIB sharding is configured, the rpd process crashes during a rare race condition where multiple threads try to initialise a single global variable. During the rpd crash and restart, all routing protocols will be impacted and traffic disruption will be seen due to the loss of routing information.
PR Number	**Synopsis**	**Category: RPD route tables, resolver, routing instances, static routes**
1687884	The traffic drop will be observed for the static route after VRRP failover when VRRP VIP is set as next-hop for that static route Product-Group=junos Severity=Major	On all Junos and Junos OS Evolved platforms, the next-hop for a static route does not refresh at PFE (Packet Forwarding Engine) after VRRP (Virtual Router Redundancy Protocol) failover when VRRP VIP (Virtual-IP) address is used as the next-hop for the static route.

1692484	Configuration check-out failed when applying "irb with inet and inet6" and "inet6.0 static route" Product-Group=junos Severity=Major	commit check for overlapping prefix will fail to commit when :: /0 static route is configured with qualified next-hop and irb interface.
1740028	Junos OS and Junos OS Evolved: RPD crashes upon concurrent deletion of a routing-instance and receipt of an SNMP request (CVE-2024-39528) Product-Group=junos Severity=Major	A Use After Free vulnerability in the Routing Protocol Daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows an authenticated, network-based attacker to cause a Denial of Service (DoS). Please refer to https://supportportal.juniper.net/JSA82987 for more information.
1746439	Route-distinguisher change leads to the route being present in rpd, but not installed in kernel/PFE Product-Group=junos Severity=Major	On Junos and Junos Evolved platforms, traffic impact will be observed when route-distinguisher change is performed for which route will be present in rpd, but not installed in kernel/PFE. This issue happens when the aggregate route is configured.
1748152	With RIB sharding configuration upon rpd restart the rpd crash will be observed Product-Group=junos Severity=Critical	On all Junos and Junos Evolved platforms, when the Routing Information Base (RIB) sharding is configured and the routing protocol process (rpd) restarts, then rpd will crash and rpd crash files will be observed.
1752133	System reboot or IPSEC restart causes routes with incorrect next hop interface to be installed in the routing table Product-Group=junos Severity=Critical	Any flap in the IPSEC (Internet Protocol Security) services or a system reboot causes interfaces in other VRFs (Virtual routing and forwarding) to get associated with the routes in a given VRF, in a topology where routes and next hops prefixes are identical across VRFs. This causes traffic loss and impacts user connectivity in IPSEC VPN scenario.
1761232	Memory spike will be observed on the system with BFD enabled Product-Group=junos Severity=Minor	On all Junos and Junos OS Evolved platforms, when Bidirectional Forwarding Detection (BFD) is enabled with any routing protocols (ex - IS-IS/OSPF), memory spikes will be observed in the system.
PR Number	**Synopsis**	**Category: Resource Reservation Protocol**
1690110	Traffic is not load-balanced when one of the next-hop LSP is down Product-Group=junos Severity=Major	On all Junos and Junos Evolved platforms, in the multi-LSP next-hop load-balance scenario, in case any one of the label-switched path (LSP) is down, the traffic will not be load-balanced to the rest of the LSPs, due to the weight of LSP next hops not being set correctly.
1694777	Restarting FPC or router reboot might causes some CCC interfaces to go down due to a 'Remote CCC down' Product-Group=junos Severity=Major	On all Junos and Junos OS Evolved platforms, if CCC (Circuit Cross-Connect) is configured to use a label-switched-path such as IGP routed, i.e., no-cspf and no strict ERO (Explicit Route Object) configuration, then restarting egress CCC node or restarting FPC on the egress CCC node containing remote-interface-switch configuration multiple times may cause CCC to remain stuck in remote-if-down state, resulting in loss of traffic. (The knob 'remote-interface-switch' is configured on the egress LER of the RSVP-TE LSP (Resource Reservation Protocol-Traffic Engineering label-switched-path) which binds the LSP terminating on the node to a local interface).
1703424	Pathtear message is not forwarded by PLR to merge point which is causing data plane blackholing Product-Group=junos Severity=Major	On all Junos and Junos OS Evolved platforms, the PLR (point of local repair) is not sending the pathtear message when the merge point supports the enhanced FRR while the route reaching the neighbor is using a shortcut route under MVPN (Multicast Virtual Private Network) configured scenario.
1713392	PathErr with RoutingProblem error code generated unexpectedly during dual failure local repair Product-Group=junos Severity=Major	When an LSR acts as a Point of Local Repair (PLR) as well as a Merge Point (MP) for an LSP during a double failure scenario, the LSR incorrectly originates one or two PathErr messages with RoutingProblem (code=24/2) instead of originating PathErr with NotifyError (code/subcode=25/3). This will not cause any service impact if the ingress LER would not react adversely to RoutingProblem error (code=24/2).
1732862	Junos OS and Junos OS Evolved: Memory leak due to RSVP neighbor persistent error leading to kernel crash (CVE-2024-39560) Product-Group=junos Severity=Major	An Improper Handling of Exceptional Conditions vulnerability in the routing protocol daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows a logically adjacent downstream RSVP neighbor to cause kernel memory exhaustion, leading to a kernel crash, resulting in a Denial of Service (DoS). Please refer to https://supportportal.juniper.net/JSA83020 for more information.

1744225	Bypass LSP traversing Flood-Reflector Cluster unexpectedly changes TE next-hop on transit node Product-Group=junos Severity=Major	On a FR-Cluster (Flood-Reflector-Cluster) Ingress node, the ERO (Explicit Route Object) of the transit bypass LSP (Label Switched Path) was expanded and a PATH message was sent to the computed next-hop. - Before the RESV was received on this node for this LSP, there was a NH (next-hop) flash event that resulted in the ERO expansion being recomputed and a PATH message was sent to the newly computed next-hop. This resulted in stale state downstream.Fix:The ERO expansion would not have been 'recomputed' if the LSP was UP at this transit node. The fix is to prevent re-computation from happening if the LSP hasn't come UP yet and ERO expansion has already been done. This issue is seen on All Junos and Junos Evolved platforms and traffic drop happens in bypass LSP scenario.
1756096	In-place-lsp-update failure causing ungraceful tear down of LSP Product-Group=junos Severity=Major	On Junos and Junos Evolved platforms, when the egress label edge router (LER) receives ResvErr from the upstream hop, the egress LER will tear down the reservation, disrupting the traffic carried over the label-switched path (LSP). The issue will happen when "in-place-lsp-bandwidth-update" is configured for the LSP on the ingress LER, or "node-link-protection" is configured for the LSP on the ingress LER and "no-enhanced-frr-bypass" is configured on all LSRs.
PR Number	**Synopsis**	**Category: RPD API infrastructure**
1710274	Next Hop counts are not as expected Product-Group=junos Severity=Critical	Next Hop counts are not as expected
PR Number	**Synopsis**	**Category: SW PRs for SCBE3 chassisd**
1745442	Traffic impact is observed on Junos MX platforms due to the chassisd crash Product-Group=junos Severity=Major	On Junos MX240/MX480/MX960 platforms with SCBE3 (Enhanced Switch Control Board), when RE (Routing Engine) is switched over by any event, the chassisd crash is seen on the new master RE due to which all the line cards will reset and the traffic will be impacted.
PR Number	**Synopsis**	**Category: Scuba chassis software**
1743686	Due to SPMB restarts in the middle of the FPC boot process, FPC wont come up Product-Group=junos Severity=Major	On MX2010 or MX2020 platforms, SPMB restarts during the FPCs boot process will cause some FPCs to boot with their MICs stuck in an "offline" state.
PR Number	**Synopsis**	**Category: Issues related to control plane security**
1781732	Junos OS and Junos OS Evolved: Impact of Terrapin SSH Attack (CVE-2023-48795) Product-Group=junos Severity=Major	An Improper Validation of Integrity Check Value vulnerability in OpenSSH before 9.6 of Juniper Networks Junos OS and Junos OS Evolved allows a remote attacker to bypass integrity checks such that some packets are omitted (from the extension negotiation message), and a client and server may consequently end up with a connection for which some security features have been downgraded or disabled, aka the Terrapin Attack. Please refer to https://supportportal.juniper.net/JSA76462 for more information.
PR Number	**Synopsis**	**Category: Generic platform and infra issues for MS-MIC and MS-MPC(XLP)**
1743031	The picd process crashes when executing the CLI command "show service sessions/flows" or "clear service sessions/flows" Product-Group=junos Severity=Major	On MX platforms with MS-MPC/MS-DPC, when the system is busy in the creation/deletion of sessions results in the picd process crashes for executing the CLI command "show service sessions/flows" or "clear service sessions/flows" aggressively (executing CLI command in 5-10 secs iteration).
1750823	The mspmand daemon crashes causing traffic loss Product-Group=junos Severity=Major	On Junos platforms with MS-MPC (Multiservices Modular Port Concentrator) like MX240, MX480, MX960, MX2008, MX2010 and MX2020, mspmand daemon (Multiservices PIC Manager Daemon) crash can be observed which causes traffic loss.
1752132	The mspmand process crashes when MPLS VRF Route	Jflow maintains the VRF table information for all the families and the routes

	table is not present for a MPLS route and MPLS route is deleted Product-Group=junos Severity=Major	present under that VRF. This information is sent by RPD to JFlow. This issue is seen when MPLS VRF table is not present for a MPLS route and we try to delete the MPLS route.
PR Number	**Synopsis**	**Category: SFW, CGNAT on MS-MIC/MS-MPC (XLP)**
1706171	PFE crash observed during deletion of service-set Product-Group=junos Severity=Major	When deleting a service-sets configuration, the PFE (Packet Forwarding Engine) may restart on MX platforms with MS-MPC (Multiservice-Modular Port Concentrator). This leads to traffic loss.
PR Number	**Synopsis**	**Category: Bug and Review Tracking for Segment routing traffic eng**
1683003	The policy-multipath route inherits the attributes of active-route but does not undergo resolution, causing an incorrect metric value Product-Group=junos Severity=Major	When an active path undergoes resolution with policy-multipath configured, policy-multipath routes are generated which inherit the attributes of active-route and do not undergo route resolution.
1720031	The rpd process crash will be observed while creating/updating the PCEP tunnel Product-Group=junos Severity=Major	On Junos and Junos OS Evolved platforms, when SR (Segment Routing) PCEP (Path Computation Element Protocol) provisional tunnel is configured along with the template but the template has delegation configured, then the PCEP update message received for creating/updating tunnels is causing the rpd process crash and tunnel creation/update will fail for PCEP provisional tunnel.
1737119	The traffic blackhole will be observed when the SRTE shortcut is configured Product-Group=junos Severity=Major	On Junos platforms, when the MPLS (Multiprotocol Label Switching) packet reaches the destination router, it will have a label that is unknown to the destination router due to a label POP operation miss at the ingress router resulting in the traffic black hole in the scenario SR-MPLS (Segment Routing With Multiprotocol Label Switching) + traffic engineering shortcut is configured.
PR Number	**Synopsis**	**Category: SRX Argon module**
1757794	AAMW hyper scan goes to lock state during reload Product-Group=junos Severity=Major	On all SRX platforms, AAMW(advanced-anti-malware) hyperscan goes to a lock state during reload. When there is a reconnect or restart of AAMW service there is a possibility depending on the timing or reload/reconnect that AAMW may crash due to hitting a lock condition.
PR Number	**Synopsis**	**Category: Remote Access VPN issues on SRX**
1721936	Junos OS: SRX Series: flowd will crash when "tcp-encap" is enabled and specific packets are received (CVE-2024-21606) Product-Group=junos Severity=Major	A Double Free vulnerability in the flow processing daemon (flowd) of Juniper Networks Junos OS on SRX Series allows a network-based, unauthenticated attacker to cause a Denial of Service (DoS). Please refer to https://supportportal.juniper.net/JSA75747 for more information.
PR Number	**Synopsis**	**Category: security-intelligence feature on SRX**
1756331	Crash files will be observed on SRX platforms Product-Group=junos Severity=Major	On SRX and vSRX platforms, crash files will be observed causing Flexible PIC Concentrators (FPCs) to reboot, when performing a DNS statistics show command without having the Domain Name System (DNS) secintel profile configuration.
PR Number	**Synopsis**	**Category: SRX branch platforms**
1594014	During reboot, "warning: requires 'idp-sig' license" can be seen on the screen even when the device has valid license Product-Group=junos Severity=Major	If a device is rebooted manually or reboots for any other reason, The following messages can be seen on the boot up screen even when the device has valid license and proper configuration to use the features like IDP/UTM
1661816	fxp0 works under disable state in SRX300 Product-Group=junos Severity=Major	SRX300 runs in HA mode, fxp0 could be unexpectedly UP even though "disable" is configured.

1709013	Kernel panic on Junos 21.2 and later platforms Product-Group=junos Severity=Major	On Junos 21.2 and later (FreeBSD) platforms, kernel panic was seen.
1738271	"Minor Autorecovery information needs to be saved" alarm is not displayed after zeroize Product-Group=junos Severity=Major	On SRX Branch platform, "Minor Autorecovery information needs to be saved" alarm is not displayed after running zeroize command
1739520	Random physical interfaces doesn't come up after a reboot Product-Group=junos Severity=Major	On SRX345, some interface ports couldn't able to get correct medium (FIBRE or COPPER) sometimes after multiple reboot due to that SFP optics inserted may not come up after a reboot.
1746202	Kernel CPU temperature becomes high and the flowd process crashes with dual VLAN tag configured Product-Group=junos Severity=Major	On all SR3xx platforms having Q-in-Q tunnelling on VPLS (Virtual Private Local Area Network Service) over GRE (Generic Routing Encapsulation) tunnel, it is seen that due to dual VLAN (Virtual Local Area Network) tag configuration, the kernel CPU (Central Processing Unit) temperature becomes high along with the flowd process getting crashed.
1770303	Inter and intra VLAN traffic drop can be seen on the SRX branch series Product-Group=junos Severity=Major	On all Junos SRX branch series devices, intra and inter-VLAN (Virtual Local Area Network) traffic drop will be seen when the devices are running in ethernet-switching mode and STP(Spanning Tree Protocol) is configured on the respective interface for the VLANs.
1776400	The Wifi MPIM card will be down upon upgrading the device Product-Group=junos Severity=Major	Upon upgrading the Junos SRX platform which is acting as a WAP (wireless access point) or WLAN (wireless LAN) installed with a Wi-Fi MPIM (Mini Physical Interface Module) card, the card is not working. This will tear down the Wi-Fi client sessions, impacting the services.
1776656	Interfaces stay down when 1G SFP fiber transceiver connected to SRX380 platform Product-Group=junos Severity=Major	Ports are staying down on SRX380 platform with 1G SFP fiber transceiver while trying to connect to a device that doesn't support auto-negotiation and/or having hard-coded speed and duplex setting
PR Number	**Synopsis**	**Category: SRX5XX platform**
1514925	Junos OS: An unauthenticated attacker with local access to the device can create a backdoor with root privileges (CVE-2023-44194) Product-Group=junos Severity=Minor	An Incorrect Default Permissions vulnerability in Juniper Networks Junos OS allows an unauthenticated attacker with local access to the device to create a backdoor with root privileges. Please refer to https://supportportal.juniper.net/JSA73158 for more information.
1634965	[SRX] SRX550HM interfaces LED of ge-0/0/6-9 will auto turn off after device bootup some minutes Product-Group=junos Severity=Major	SRX550HM interfaces LED of ge-0/0/6-9 will auto turn off after device bootup some minutes.
PR Number	**Synopsis**	**Category: SSL Proxy functionality on JUNOS**
1752678	Large TLS1.3 session tickets to an SRX SPC3 device result in srxpfe crash Product-Group=junos Severity=Major	On SRX platforms with SPC3 card with SSL (Secure Sockets Layer) Proxy enabled, the srxpfe process crash will be observed impacting the traffic flow when the system is unable to handle large TLS1.3 (Transport Layer Security) session tickets (bigger than 1682 bytes) received from access sites.
1753540	The flowd process will crash due to memory stress Product-Group=junos Severity=Major	On Junos based SRX platforms in a low memory condition, the flowd process will crash because of memory corruption and crash files will be observed. Traffic flow will be impacted till the time flowd restarts.
PR Number	**Synopsis**	**Category: MPC7/8/9 Interface Issues**
1682962	Auto-negotiation is not getting reflected on the MPC7E-10GE line card Product-Group=junos	On all MX platforms with MPC7E-10GE line card, auto-negotiation will not be set properly when changing the port speed from 10GE to 1G on a port with auto-negotiation configured. The port remains down until the commit is done

	Severity=Major	separately for changing the port speed.
PR Number	**Synopsis**	**Category: Stout card (MPC7) fabric issues**
1764457	Traffic drop observed at the source pfe when the destination line card has fabric link error Product-Group=junos Severity=Major	On all Junos and Junos Evolved platforms, when data traffic is sourced from line cards like MPC1-9 and there is a link error at the destination PFE (Packet Forwarding Engine) end, traffic is dropped at the source PFE end.
PR Number	**Synopsis**	**Category: Stout cards (MPC8, MPC9) fabric issues**
1747893	MX2k Platform: frequent fabric plane Check state reported due to remote destination timeouts Product-Group=junos Severity=Major	Upon some crc errors on fabric links, fabric destination timeouts are reported more frequent. Once there is a fabric request timeout, the system will attempt auto recovery. Since the periodic detection logic ran twice for 500msec period and 60msec period, it reported fabric destination timeout too aggressive. The additional 60msec period is targeted to detect a condition if user removed SFB board ungracefully. This exposure is specific to MX2K Platforms only
PR Number	**Synopsis**	**Category: MX10002 Platform SW - Platform s/w defects**
1755585	VMHost memory exhaustion results in image installation failure and brings down the RE during the upgrade Product-Group=junos Severity=Major	On VM Host platforms, if the available memory is lower than 7G, the VM Host software install fails and an error message is displayed regarding the lack of space. If a reboot is followed after such failed installation, the RE (Routing Engine) goes dead or boots from secondary disk.
PR Number	**Synopsis**	**Category: MX10003/MX204 Linux issues (including driver issues)**
1753908	Device crash and control plane traffic gets impacted on Junos platforms Product-Group=junos Severity=Major	On all Junos platforms, due to a timing issue, when monitor traffic is enabled on loopback interface (for debug purpose), in the presence of local TCP (Transmission Control Protocol) packet flow, it is observed that the device crashes and traffic gets impacted.
PR Number	**Synopsis**	**Category: MX10003/MX204 MPC defects tracking**
1686012	100GE interface on JNP-MIC1 TIC module may keep flapping for 1 ~ 45 minutes after a specific 3rd party peer device (NRU02 from Arista/Pluribus) is booting up. Product-Group=junos Severity=Major	100GE interface on JNP-MIC1 TIC module may keep flapping for 1 ~ 45 minutes after a specific 3rd party peer device (NRU02 from Arista/Pluribus) is booting up.
1757878	Interface using a QSA adapter with 1G speed won't work Product-Group=junos Severity=Major	On SRX1RU 4XQSFP28 and MX10003 6XQSFP28 PIC MIC cards ie BCM82328F PHY using MIC card, QSA adapter with 1G speed won't work.
PR Number	**Synopsis**	**Category: SRX-1RU platfom datapath SW defects**
1746567	Junos OS: SRX4600 Series: A high amount of specific traffic causes packet drops and an eventual PFE crash (CVE-2024-30398) Product-Group=junosvae Severity=Major	An Improper Restriction of Operations within the Bounds of a Memory Buffer vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS). Please refer to https://supportportal.juniper.net/JSA79176 for more information.
1775083	Traffic drop observed right after boot up on Junos SRX 4600 platforms Product-Group=junosvae Severity=Major	On SRX 4600 platforms running the Field Programmable Gate Array (FPGA) firmware versions 163, 165, 171, 175 the Packet Forwarding Engine (PFE) may experience a 25% drop in performance after bootup.
PR Number	**Synopsis**	**Category: SRX-1RU platfom related protocol, QoS, filtering features et**
1748971	SRX4600 misleading Fan speed syslog output after removing or inserting one Fan tray unit	On SRX4600, misleading Fan speed syslog is generated after removing or inserting one Fan tray unit.

	Product-Group=junos Severity=Minor	
PR Number	**Synopsis**	**Category: MX10003/MX204 Timing/Sync-E issues tracking**
1773747	Alarms tied to lclksyncd application failure are seen after a downgrade of Junos Product-Group=junos Severity=Major	Alarms tied to lclksyncd application failure are seen after a downgrade of Junos
PR Number	**Synopsis**	**Category: ZT/YT pfe qos software issues**
1705353	Syslog "[Error] COS SCHED : Token mismatch during Q stats update" seen during config change or when subscriber sessions are going down. Product-Group=junos Severity=Major	When a COS scheduling node (IFD/IFL/IFLSET) is being deleted due to config change or when subscriber sessions are going down, the following log maybe seen sometimes right after commit: "[Error] COS SCHED : Token mismatch during Q stats update."
PR Number	**Synopsis**	**Category: ZT/YT pfe firewall software**
1706966	Stray firewall filter instances may be left on the FPC after the configuration is reverted Product-Group=junos Severity=Major	Stray firewall filter instances may be left on the FPC after the configuration is reverted. This problem is seen with consecutive commits tied to filter add/remove with no delay.
1715504	Traffic is leaking during a filter change Product-Group=junos Severity=Critical	On all EX92XX and MX platforms having MPC10, MPC11 and LC9600 cards, traffic is leaking through a scale filter configuration change.
1722776	The filter will not work as configured upon changing the "physical-interface-policer" parameters Product-Group=junos Severity=Major	On Junos platforms with MPC10/MPC11/LC-9600 linecard, whenever the "physical-interface-policer" parameters are changed for the "physical-interface-filter" having more than one type of policers (i.e two-color, three-color, Hierarchical policer), the alarm "Potential slow peers are: XDPC2" is generated and the filter will not work as configured and the changes will not reflect in the data plane.
1733724	Inline Services MAP-E is failing on MPC10 after configuration modification Product-Group=junos Severity=Major	On MX platform with MPC10 line card, when there is a modification in configured inline-services under Mapping of Address and port Encapsulation (MAP-E) which results inline MAP-E feature will not work and it causes traffic loss.
1738548	DHCP offer is dropped at MX and specific EX platforms when an lt interface is used as the transport Product-Group=junos Severity=Major	On MX and EX92_XX platforms, the DHCP offer will be dropped when LT interface is used to reach the DHCP server. DHCP relay will not work as expected due to this issue.
1743930	Traffic drop is observed after the addition or removal of the "filter-specific" knob under the policer Product-Group=junos Severity=Major	On MX platforms with MPC10, MPC11 and JNP10K-LC9600 linecards, when both regular & hierarchical/tricolor policer is configured on the logical interface (ifl), after the addition or removal of "filter-specific" knob under this combination of policer traffic drop is observed.
1757636	Traffic blackholing is observed on certain MX & EX92XX based platforms after committing specific filter configurations Product-Group=junos Severity=Critical	On MX platforms with MPC10, MPC11, LC9600, MX304, and EX92xx platforms, when a firewall filter is attached to an AE interface a dummy filter will be installed automatically on line cards that don't have any child leg in the AE interface to save the ASIC resources. Later if the same filter is attached to any physical / AE interface of that line card or local child leg is added then the filter is changed from dummy to actual but the relation is broken between the filter instance (H/W Instance) and the filter Template (Definition) results in traffic blackholing.
1775551	The error messages are observed on MX platforms for ICMP packets Product-Group=junos Severity=Major	The MPC10 reporting error messages; aftd-trio: [Error] DFWCOMMON Packet buffer doesn't have sufficient size to decode src and dst ports Packet buffer size:2 Src and dst ports size:4
PR	**Synopsis**	**Category: ZT/YT pfe l3 forwarding issues**

Number		
1713958	Unexpected load balancing of packets having GRE header Product-Group=junos Severity=Major	On all Junos and Junos Evolved platforms, incorrect load balancing of packets is observed when the transit packet with GRE (Generic Routing Encapsulation) header having any header fields (checksum, sequence number, etc) other than GRE key is present.
1719763	Incorrect forwarding lookup in Packet Forwarding Engine on MX platforms with MPC10E/11E/LC9600/MX304-LMIC16 line cards in an L2circuit Scenario with Flow-Label and Control-Word enabled Product-Group=junos Severity=Major	On Junos MX platforms, packet drop is seen in Layer 2 circuit when flow-label is enabled along with control-word and the egress Provider Edge (PE) core facing interface is on MPC10E/11E/LC9600/MX304-LMIC16. Certain flows will get punted to RE (Routing Engine) instead of getting forwarded.
1731587	Telemetry data not sent for /junos/services/label-switched-path/usage/ on MPC11E cards Product-Group=junos Severity=Minor	Telemetry Stats are not visible for MPLS LSP(RSVP Based) when the core interface is MPC11/MPC10.
1755950	The aftd process crashes on MX304 continuously when turning up BGP neighbours with no LMIC card on slot 0 Product-Group=junos Severity=Major	On MX304 platforms, when the slots 0 is empty or the LMIC card on slot 0 is inactive (PFE0 is inactive) and the LMIC card is active on slot 1 or 2, the aftd process crashes continuously when BGP neighbours are turned up. This leads to complete loss of traffic till the aftd process restarts.
1759899	The system crashes due to the deletion of the basic IP configuration Product-Group=junos Severity=Critical	On Junos MX devices with MPC10, MPC11, LC9600 line cards and MX304 platforms, the deletion of the basic Internet Protocol (IP) configuration was resulting in the system crash. Apart from this, any rollback/configuration delete that results in a receive next-hop (NH) free/delete have the possibility of ending up in a system crash scenario.
1774127	Memory leak for deactivation/activation of SCU Product-Group=junos Severity=Major	On MX platforms with MPC10, MPC11, LC9600, and MX304-LMIC16, the heap memory leaks every time the SCU (source-class-usage) policy is removed i.e. removed and re-applied resulting in restart of the line card. Heap leak is proportional to the number of source classes or indices being removed by related policy.
PR Number	**Synopsis**	**Category: ZT/YT pfe, vpls, mesh group software**
1755161	The interface stats interrupt may be lost resulting in stats not getting updated Product-Group=junos Severity=Major	On certain line cards, if link up/down interrupts and stats interrupt at the same time, stats interrupt may be lost resulting in stats not getting updated. This issue will not have any impact on the traffic, only the statistics will not be updated.-Seen on MPC10/ MPC11 / MX304 / LC4800 / LC9600 -If link up/down interrupts and stats interrupt at the same time, stats interrupt may be lost resulting in stats not getting updated.- This issue only impacts interface stats. It DOESN'T have any real traffic impact Issue can be confirmed byStats stop updating/working. The counts will be stuck as seen in the below command:start shell user root vty fpcXfpcX:pfe>show cda toe intr-count pfeId toeId 0. <<< N is 0-2 on MPC10, 0-7 on MPC11, 0-11 on LC9600, 0-5 on MX304 and LC4800
PR Number	**Synopsis**	**Category: Issues related to broadband edge apps (PPP, DHCP) on Trio ch**
1747009	Traffic from subscribers will be dropped by Junos based MX platforms Product-Group=junos Severity=Major	On Junos based MX platforms in enhanced subscriber management scenario, with 'routing-services' and 'rpf-check' feature enabled all traffic from subscribers will be dropped.
PR Number	**Synopsis**	**Category: Trio pfe qos software**
1726698	On certain Junos MX platforms queue buffer-size temporal computation is not happening correctly Product-Group=junos Severity=Major	On certain Junos MX platforms, if a queue's buffer size is configured as temporal value and the transmit-rate/guaranteed-rate is not configured as absolute value at COS (Class of Service) schedulers or traffic-control-profile level, then a very low queue depth buffer gets allocated to the queue. This will lead to aggressive tail-drops on the queue.
1777932	Traffic blackhole on the egress interfaces hosted on hyper-mode enabled FPC with flexible-ethernet-services	On MX platforms, when flexible-ethernet-services encapsulation is enabled only a single egress feature is installed, and the hyper-mode IFL (logical interface)

	encapsulation configured Product-Group=junos Severity=Major	egress optimization code kicks in when the IFL family has only 1 egress feature. In this case, policy-map instructions are executed using optimised wan_out NH (Next-Hop), instead of the regular wan_out NH. Currently, the opcode sanity check in the entry_set_policy_map instruction only checks for the regular wan_out NH fields. Added new opcode sanity checks to validate the optimized wan_out NH fields.
1783261	Parity error Alarm in Queing Packet Reader block needs to be moved from severity Major to Minor Product-Group=junos Severity=Major	Alarms EA_PR_PROTECT_FSET_1_REG_DETECTED_SHAPE_RAM, XQSS_CMERROR_PR_PROTECT_FSET_1_REG_DETECTED_OPAQUE, XQSS_CMERROR_PR_PROTECT_FSET_1_REG_DETECTED_CD and XQSS_CMERROR_PR_PROTECT_FSET_1_REG_DETECTED_EXP_ST to Minor errors , as there is a code logic in place to report XQSS_CMERROR_CORRECTABLE_MEM_ERR Major error when the number of correctable errors crosses a threshold of 32 events per week.
PR Number	**Synopsis**	**Category: Trio pfe stateless firewall software**
1682164	Traffic drop is seen after configuring fast-lookup-filter Product-Group=junos Severity=Major	On MX platforms with specific line cards, when fast-lookup-filter (FLT) is used on a highly scaled device, a packet processing loop in PPC will corrupt the internal next-hop lookup, causing a traffic drop.
1724563	Traffic drop would be observed while restarting the chassis-control Product-Group=junos Severity=Minor	On MX platforms with MPC1 to MPC9 line cards, while restarting chassis-control, the line card crashes as the watchdog timer panics due to an internal thread being too busy seemingly finding if a particular term-based filter has a term with then port-mirror-instance <> for a particular instance name.
PR Number	**Synopsis**	**Category: TRIO Interface based services**
1730840	PFE crashes when "exception-reporting category packet-errors" is configured on MX, EX9K and SRX5K platforms Product-Group=junos Severity=Major	On Junos MX series, EX9K and SRX5K platforms, configuring the "exception-reporting category packet-errors" knob leads to Packet Forwarding Engine (PFE) crash.
PR Number	**Synopsis**	**Category: Trio pfe bridging, learning, stp, oam, irb software**
1718372	Remote EVPN router is not receiving ARP packets for double-tag VLAN when sender is sent a packet from MPC10 and MPC11 line card Product-Group=junos Severity=Major	On MX platform with MPC10, MPC11 and JNP10K-LC9600 linecard, when Ethernet VPN (EVPN) is set up in an end-to-end double-tagged Virtual LAN (VLAN) case, ARP requests are sent from the MPC10/MPC11 or JNP10K-LC9600, but the remote EVPN router is not getting ARP packets as a result, which causes problems with the mac-ip in the end-to-end double-tagged VLAN case.
1724925	Traffic loss observed for packets over IRB over LT Product-Group=junos Severity=Major	On all Junos MX with MPC1-9 and EX9K platforms, traffic loss will be seen when a L3 domain (either a VRF or default routing-instance) with an underlying IRB (Integrated Routing and Bridging) interface is stitched to another L2 domain (VPLS domain/ L2circuit/ bridge domain) with a LT (Logical Tunnel) interface acting in the access mode.
1728922	CFM delay-measurement fail to send out DMM messages, when CFM is configured on MPC5EQ PIC 1 Product-Group=junos Severity=Major	when configure CFM delay-measurement using MPC5EQ PIC1 interface, cfm delay-measurement fail, DMM messages cannot be sent out from MPC pfe.
1729970	L2-Trans: pm_soam_frame_rx count is not incrementing as expected Product-Group=junos Severity=Critical	L2-Trans: pm_soam_frame_rx count is not incrementing as expected
1731564	VPLS traffic gets blackholed by qualified-bum-pruning mode Product-Group=junos Severity=Major	On all MX and EX9K platforms, qualified-bum-pruning-mode completely blackholes VPLS (Virtual Private LAN Service) traffic with network-services configured in enhanced-ip mode.
1736667	Intermittent flooding of traffic every 40 sec Product-Group=junos Severity=Major	On MX/EX92K Junos platforms with line cards running MPC families up to MPC9, Layer2 unicast traffic flow sent on FPC where Pseudowire Subscriber Interfaces (PS interface) is not anchored and the packet contains DMAC as one of the MACs learned behind that PS IFL. Packets with DMAC as that of the Mac learned behind

		PS IFL is getting flooded from the FPCs where PS IFL is not anchored every 40sec. The impact is that every 40sec traffic sent towards a known MAC will be flooded as this destination MAC was unknown. This traffic shouldn't be flooded arriving at incorrect destinations.
1740606	Host communication does not work in EVPN-L2VPN-CCC setup Product-Group=junos Severity=Major	On Junos MX platforms, in Ethernet Virtual Private Networks-Layer 2 Virtual Private Networks-Circuit Cross-Connect (EVPN-L2VPN-CCC) setup, the integrated routing and bridging (IRB) interface over access logical tunnel (LT) interface is configured, it is sending vlan tagged packet on the access port and not removing it causing the host communication to break.
1743947	PFE will wedge for RVTEP connectivity having unilist VENH Product-Group=junos Severity=Major	On all Junos MX platforms, in a rare scenario when the Remote Virtual Tunnel Endpoint (RVTEP) IP routes are pointing to unilist Virtual Extensible Local Area Network (VXLAN) Encapsulated Nexthop (VENH) and all the underlay ports of the VXLAN tunnel go down, then the Packet Forwarding Engine (PFE) will detect traffic congestion and will wedge with CM_Error alarms.
1751846	[MX480/MX240] Multicast ping ff02:: 1 cannot perform reply on MX240/480 platform from MX204 via VXLAN Product-Group=junos Severity=Major	When MX204 and MX240/MX480 connected over static VxLAN with IPv6 underlay and IPv6 configured on IRB interface, Multicast ping with IPv6 address will fail while trying multicast ping with IPv6 address from MX204, ICMP response is not received from MX240/MX480 when other FPC is online.
1759454	Fusion Provider Edge Satellite LAG CFM not working with peers Product-Group=junos Severity=Major	On all Junos fusion platforms, CFM (Connectivity Fault Management) session will not come up when configured on ae (aggregated ethernet) interface. However there is no traffic impact only CFM session is not coming up.
1772733	In EVPN-MPLS/EVPN-VxLAN Multi-Home Active/Active scenario, random packet drops are observed Product-Group=junos Severity=Major	On all Junos MX platforms, in Ethernet Virtual Private Network Multiprotocol Label Switching (EVPN-MPLS)/ Virtual eXtensible Local-Area (EVPN-VxLAN) Network Multi-Home Active/Active scenario, random packet drops will be observed on the Non-Designated-Forwarder for ARP-REPLY generated in response to ARP-REQUEST received for Virtual-Gateway-Address defined on the IRB interface.
PR Number	**Synopsis**	**Category: Trio pfe l3 forwarding issues**
1700203	DHCP offer requests are dropped while routed towards different VRFs of transit router Product-Group=junos Severity=Major	On all Junos platforms with route leaking and no-snoop configuration, DHCP (Dynamic Host Configuration Protocol) offer requests could be dropped while traversed to different VRFs (Virtual Routing and Forwarding) from default RI (Routing Instance).
1763890	ISIS adjacency failed to be up if gr- interface and underlay interface on same pfe instance Product-Group=junos Severity=Major	When gr and wan interface are on same pfe, when the ISISoGRE packet is received, l2 header doesnt get stripped out leading to host-path dropping the packet. As a result ISISoGRE doesnt come up. When the interfaces are on different pfe, what gets sent out on fabric from source PFE is L3 payload and eventually it works.
PR Number	**Synopsis**	**Category: Trio LU and LUSS SW driver**
1735490	Junos OS: MX Series: Continuous subscriber logins will lead to a memory leak and eventually an FPC crash (CVE-2024-39539) Product-Group=junos Severity=Critical	A Missing Release of Memory after Effective Lifetime vulnerability in Juniper Networks Junos OS on MX Series allows an unauthenticated adjacent attacker to cause a Denial-of-Service (DoS). Please refer to the https://supportportal.juniper.net/JSA82999 for more information.
PR Number	**Synopsis**	**Category: Trio pfe mpls- lsps, rsvp, vpns- ccc, tcc software**
1757984	Memory exhaustion leading to FPC core with auto-policing enabled MPLS with Multicast P2MP Product-Group=junos Severity=Major	On MX platforms with MPC1/MPC2E/MPC7E/MPC8/MPC9E, when auto-policing is enabled under MPLS (Multiprotocol Label Switching) with Multicast P2MP (Point-to-Multipoint) and MVPN (Multicast Virtual Private Network) route churn, traffic impact is observed due to heap memory leak for which FPC gets stuck.
PR Number	**Synopsis**	**Category: Trio pfe multicast software**
1686068	Disabling PFE triggers the memory leak which may cause	On Junos MX platforms with specific line cards, when PFE (Packet Forwarding

	FPC to crash Product-Group=junos Severity=Major	Engine) is disabled, scenarios like multicast receiver join/leave that result in allocation and de-allocation of memory on disabled PFE can cause a memory leak. This is because memory is allocated on the disabled PFE, but not freed.
PR Number	**Synopsis**	**Category: Trio pfe sampling, services plumbing**
1759592	Reverse traffic failing for interface-style stateful firewall on MPC5 line cards Product-Group=junos Severity=Major	On all Junos MX platforms with MPC5 linecard, when we configure interface-style SFW (stateful firewall) and applying the service-set on interface, reverse traffic is not getting processed.
PR Number	**Synopsis**	**Category: XMCHIP Related SW Issues**
1724841	Memory initialization and scrub operation using PFE's fails Product-Group=junos Severity=Critical	On MPC5/6/7/8/9 line cards, the memory initialization/scrub operation using PFE's (Packet Forwarding Engine) may fail in very rarely scenario. If memory scrub at line card initialization fails we may see initialization errors and a large number of PFE traps. Partial to full service impact depending on which event failed.
PR Number	**Synopsis**	**Category: DDos Support on MX**
1615357	The snmpd CPU utilization reaches 100% with error logs Product-Group=junos Severity=Minor	On all MX platforms, sending SNMP traffic at bandwidth greater than 20000pps observed DDoS (Distributed Denial of Service) violations & error logs with 100% snmpd CPU utilization.
PR Number	**Synopsis**	**Category: MGD issues being found in cMGD environment**
1723551	On containerised platforms, change in configuration is not propagated to existing CLI sessions. Product-Group=junos Severity=Major	When configuration change is committed, this change is not informed to existing CLI sessions on containerised platforms like cRPD. So, user needs to close existing CLI sessions and use new CLI sessions after configuration change is committed.
PR Number	**Synopsis**	**Category: Ephemeral Database**
1610713	The rpd crash will be observed post ephemeral database configuration commit sync Product-Group=junos Severity=Major	On Junos and Junos Evolved platforms, post ephemeral database configuration commit sync leads to a state mismatch between master and backup.
1751141	Load replace via XML NetConf will not work Product-Group=junos Severity=Major	On all Junos and Junos OS Evolved platforms, the load replace operation through XML NetConf will fail.
PR Number	**Synopsis**	**Category: UI Infrastructure - mgd, DAX API, DDL/ODL**
1680065	Python scripts might fail with cscript core due to missing package Product-Group=junos Severity=Major	On platforms with arm architecture, Post python3 upgrade, the python scripts might fail with cscript core due to missing libffi package. This issue has no impact on traffic.
1718063	After deleting commit scripts with transient changes, the changes do not take effect Product-Group=junos Severity=Major	On Junos OS Evolved ACX7100-32C / ACX7100-48L / ACX7509 / PTX10001-36MR / PTX10003 / PTX10004 / PTX10008 / PTX10016 platforms, when a commit script with transient configurations is deleted, daemon does not see the change after commit.
1726731	After the device reboot BGP sessions configured with authentication will be down Product-Group=junos Severity=Major	On all EX4100 platforms, after the device reboot, BGP (Border Gateway Protocol) peers with authentication remain down as the keyadmin utility is not invoked causing the kernel database to not populate with MD5 configuration.
1740289	The 'load replace' operation might result in mustd and mgd crash	On Junos and Junos Evolved platforms with 'apply-group' configured, the mustd and mgd processes might crash when the 'load replace' operation is performed.

	Product-Group=junos Severity=Major	When this happens, 'apply-groups' will get deleted internally and the respective hierarchies will not be notified.
1761939	CLI users cannot access configuration mode on Junos and Junos OS Evolved platforms Product-Group=junos Severity=Major	On Junos and Junos OS Evolved platforms due to the mgd(Management Daemon) process not releasing commit lock, CLI users cannot change the configuration. CLI users cannot access configuration mode when maximum edit sessions limit is reached in this state. There is no service impact due to this issue.
1771991	RSI is more than 3.7 GB Product-Group=junos Severity=Major	The CLI command output of "show system processes extensive" should not have an 'srd' entry on PTX.
1772201	unexpected commit error - error: VLAN-ID must be specified on tagged ethernet interfaces Product-Group=junos Severity=Major	unexpected commit error like 'error: VLAN-ID must be specified on tagged ethernet interfaces', due to 'commit check' reset internal flag incorrectly after load overide configuration in rare condition.
PR Number	**Synopsis**	**Category: Issues related to NETCONF**
1702241	Junos OS and Junos OS Evolved: A low-privileged user can access confidential information (CVE-2024-21615) Product-Group=junos Severity=Critical	An Incorrect Default Permissions vulnerability in Juniper Networks Junos OS and Junos OS Evolved allows a local, low-privileged attacker to access confidential information on the system. Please refer to https://supportportal.juniper.net/JSA75756 for more information.
PR Number	**Synopsis**	**Category: Web-Management UI**
1776688	High storage is reported in /var/jail/log due to http.log and http-trace.log on all Junos platforms Product-Group=junos Severity=Major	Disk usage will be high in /var/jail/log due to http.log and http-trace.log on all Junos platforms. Further install will be blocked until this folder is cleaned up.
PR Number	**Synopsis**	**Category: QFX RCB issues**
1589942	The management interface speed is reflected as 10G instead of 1G Product-Group=junos Severity=Minor	On VMHost platforms, the management interface speed is displayed as 10G instead of 1G. There is no functionality impact. This issue needs two fixes PR1589942 and PR1636668. Make sure both are included.
1763588	Warn if insufficient space to save unbundled packages during vm image upgrade Product-Group=junos Severity=Major	If while preparing for replacement of a vm image, there is insufficient space to save copies of unbundled packages, issue a warning.
PR Number	**Synopsis**	**Category: web filterig issues**
1755998	Certain video streaming services continuously buffer when safe-search and HTTP persistent mode is enabled Product-Group=junos Severity=Major	On all SRX and NFX series platforms that support UTM (Unified Threat Management) with enhanced web-filtering, when http-persist (HTTP persistent mode) and safe-search (enabled by default) is enabled, web-filtering is unable to handle multiple HTTP requests and leads to blocking of certain http/https based web services. An end user can experience continuous buffering of HTTP/HTTPs based video streaming services.
PR Number	**Synopsis**	**Category: MX10K platform**
1784080	FPC reboot seen on MX platforms with PMB memory correctable errors Product-Group=junos Severity=Major	On all MX platforms that support MPC7/MPC8/MPC9/MX10k-LC2101/EX9200-40XS/EX9200-12QS, an unexpected FPC (Flexible PIC Concentrator) reboot may be seen along with PMB memory correctable errors. Service impact can be seen till the FPC restart completes.
PR Number	**Synopsis**	**Category: PTX/QFX100002/8/16 platform software**
1770691	PEM firmware upgrade fails on PTX installed with	On PTX platforms with JNP10K-RE, In affected version platform specific attribute

	JNP10K-RE Product-Group=junosvae Severity=Major	is missed which caused PEM firmware upgrade fail.
PR Number	**Synopsis**	**Category: VMHOST platforms software**
1658028	System hangs for 17 mins after 'request system reboot Product-Group=junos Severity=Major	Junos only reboot using "request system reboot" results in guest Hang.
1772127	After device reboot Swap memory is not displayed in the CLI command output of "show system processes extensive" Product-Group=junosvae Severity=Minor	On the Junos PTX10008 and PTX10016 platforms, Swap memory is not getting displayed in the CLI command output of "show system processes extensive". The Swap partition is deleted for certain conditions on the Junos side and the external swap partition is not getting created during the boot-up, hence this issue is happening. The issue can be avoided temporarily using a workaround method until reboots. A permanent issue fix is provided for PTX10008 & PTX10016 in the latest release.
PR Number	**Synopsis**	**Category: Virtual Private LAN Services**
1680687	The rpd crash is seen due to the creation of a new logical interface Product-Group=junos Severity=Major	On all Junos Evolved and Junos MX platforms, when a new logical interface(LSI) is created, but the configuration was deleted as the kernel failed to add the interface will lead to rpd crash.
PR Number	**Synopsis**	**Category: usf url filtering related issue**
1737670	URL-Filtering few HTTP sites are getting bypassed and redirect is not happening Product-Group=junos Severity=Major	On Junos MX series platforms with service card (SPC3, MS-MPC and MS-MIC), when the contents in the url-filter-database file are in upper case, the URL (Uniform Resource Locator) filtering fails to filter those HTTP (Hypertext Transfer Protocol) URIs (Uniform Resource Identifier) which are meant to be redirected.
1751860	Service PIC enabled with url-filtering may crash and gets into booting loop Product-Group=junos Severity=Major	On MX platforms, with service cards running url-filtering plug-in, when the domain-names are resolved with more than 10 IPv6 or IPv4 addresses, may results in service PIC crash.
PR Number	**Synopsis**	**Category: usf flow and datapath issue on SPC3**
1750634	Traffic transfer/receive is impacted for SPC3 CPU cores connected to the affected PCIe bus when the SPC3 or PIC card boots up Product-Group=junos Severity=Major	On MX and SRX platforms with SPC3 card, SPC3 (Services Processing Card 3) CPU cores connected to the affected PCIe (Peripheral Component Interconnect) bus (7 CPU cores) getting into a bad state will not transfer any traffic i.e. traffic loss during SPC3 or PIC card bootup due to incorrect register settings.
PR Number	**Synopsis**	**Category: usf service set related issues**
1779424	Junos OS: MX Series with SPC3 line card: Port flaps causes rtlogd memory leak leading to Denial of Service (CVE-2024-39550) Product-Group=junos Severity=Major	A Missing Release of Memory after Effective Lifetime vulnerability in the rtlogd process of Juniper Networks Junos OS on MX Series with SPC3 allows an unauthenticated, adjacent attacker to trigger internal events cause (which can be done by repeated port flaps) to cause a slow memory leak, ultimately leading to a Denial of Service (DoS). Please refer to https://supportportal.juniper.net/JSA83012 for more information.

22.2R3-S3 - List of Known issues

PR Number	Synopsis	Category: Software build tools (packaging, makefiles, et. al.)

1698624	cRPD: Multiple vulnerabilities resolved in 23.4R1 release Product-Group=junos Severity=Critical	Multiple vulnerabilities have been resolved in Juniper Networks Junos cRPD by updating third party software included with cRPD. Please refer to https://supportportal.juniper.net/JSA79107 for more information. *Resolved In:* junos:20.3X75-D43 junos:22.4R1-S1 junos:22.4R1-S2 junos:22.4R2 junos:23.1R1
PR Number	**Synopsis**	**Category: L2NG SFLOW feature**
1699585	On Junos platforms, after 24 days of device booting, sflow adaptive sampling may stop working. Product-Group=junos Severity=Major	On Junos platforms, anytime after 24 days of device reboot, adaptive sampling may stop working. Restarting sflowd or deactiviting/activating sflow will resolve this issue temporarily, but it can reoccur anytime again. You will need to reboot the device to ensure that this issue is not seen for next 24 days. *Resolved In:* junos:20.4R3-S6 junos:21.4R3-S3 junos:22.2R3 junos:22.3R3 junos:22.4R2 junos:23.1R1 junos:23.2R1
PR Number	**Synopsis**	**Category: EX4300 PFE**
1770410	Junos OS: EX4300 Series: Firewall filter not blocking egress traffic (CVE-2024-30389) Product-Group=junos Severity=Minor	An Incorrect Behavior Order vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS on EX4300 Series allows an unauthenticated, network-based attacker to cause an integrity impact to networks downstream of the vulnerable device. Please refer to https://supportportal.juniper.net/JSA79185 for more information. *Resolved In:* junos:21.4R3-S6
1774634	Junos OS: EX4300 Series: If a specific CLI command is issued PFE crashes will occur (CVE-2024-30384) Product-Group=junos Severity=Major	An Improper Check for Unusual or Exceptional Conditions vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS on EX4300 Series allows a locally authenticated attacker with low privileges to cause a Denial-of-Service (Dos). Please refer to https://supportportal.juniper.net/JSA79186 for more information. *Resolved In:* junos:19.1R3-S12 junos:19.2R3-S9 junos:19.4R3-S13 junos:20.2R3-S9 junos:20.4R3-S10 junos:21.2R3-S7 junos:21.4R3-S6
PR Number	**Synopsis**	**Category: EX4300 Platform**
1714117	PFEX process crash observed when device comes up after zeroize or interface configuration deletion Product-Group=junos Severity=Major	On Junos OS EX4300 and EX4300-VC platforms, if zeroize or interface configuration deletion performed, PFEX process crash will se seen when interface/device comes up and there will be traffic loss during the PFE restart. *Resolved In:* junos:20.4R3-S7 junos:21.1R3-S5 junos:21.2R3-S5 junos:21.3R3-S4 junos:21.4R3-S4 junos:21.4R3-S4-X1
1747374	SFP modules are not detected after upgrade Product-Group=junos Severity=Major	After an upgrade, the SFP modules are not detected in case of EX4300 platforms and the ports remain down impacting traffic. *Resolved In:* junos:20.4R3-S10 junos:21.2R3-S8 junos:21.4R3-S6
1749289	On EX4300, "Error requesting CMTFPC SET INTEGER" and "Error requesting SET BOOLEAN" logs may be seen after device boot up. There is no functional impact for the error messages Product-Group=junos Severity=Major	On EX4300, "Error requesting CMTFPC SET INTEGER" and "Error requesting SET BOOLEAN" logs may be seen after device boot up. There is no functional impact for the error messages *Resolved In:* junos:20.4R3-S9 junos:21.2R3-S7 junos:21.3R3-S5 junos:21.4R3-S5
1752611	The port attached to 40 DAC cable doesn't come up after software upgrade or switch reboot Product-Group=junos Severity=Major	On EX switches, if 40G DAC(Direct Attach Copper) cables with PN(Part Number) 740-038624 (QSFP+-40G-CU3M) and 740-044512 (QSFP+-40G-CU50CM) are used, links might not come up after software upgrade to Junos 21.4R3-S3 or after a switch reboot (if the switch is running Junos 21.4R3-S3). The switch ports that use these DAC cables are observed to go down after a reboot. *Resolved In:* junos:21.2R3-S7 junos:21.4R3-S6
1779410	The pfex process crash is observed when PIC is	On EX4300 or EX4300-VC, removal of a Physical Interface Card (PIC), or if the

	removed Product-Group=junos Severity=Major	software fails to detect a PIC that is installed, it can cause a crash in the pfex process. This crash can lead to high CPU usage and potentially disrupt network traffic. *Resolved In:* junos:21.4R3-S7
PR Number	**Synopsis**	**Category: EX4300 HA (GRES, NSR, NSB)**
1665562	NSSU aborted with Backup RE in an inconsistent state Product-Group=junosvae Severity=Major	On EX4300-48MP platform during NSSU (Nonstop Software Upgrade) operation, configured in VC (Virtual Chassis) mode with NSR (Nonstop-Routing) and GRES (Graceful-Switchover) configured, the Backup RE (Routing Engine) will be in an inconsistent state generating error messages and NSSU operation gets aborted. *Resolved In:* junos:20.4R3-S4 junos:21.2R3-S7 junos:21.3R3-S1 junos:21.3R3-S5 junos:21.4R3 junos:21.4R3-S4 junos:21.4R3-S5 junos:21.4R3-S6 junos:22.1R2 junos:22.1R3 junos:22.1R3-S5 junos:22.2R1 junos:22.2R2 junos:22.3R1 junos:22.4R1
PR Number	**Synopsis**	**Category: EX2300/3400 platform**
1772477	Turning port beacon LED on or OFF may not change the LED status Product-Group=junos Severity=Major	On EX2300, turning port beacon LED on or OFF may not change the LED status. There is no service impact due to this. *Resolved In:* junos:22.2R3-S4 junos:22.3R3-S3 junos:22.4R3-S2 junos:23.4R2 junos:24.2R1
PR Number	**Synopsis**	**Category: QFX VC/VCF NSSU**
1706892	Traffic loss upon switchover during NSSU when unreachable name-server is configured Product-Group=junos Severity=Major	When NSSU is attempted and an unreachable name-server is configured on the device traffic loss will be observed upon switchover. Back-up FPC takes mastership while previous Master FPC is undergoing reboot and traffic drops are seen due to PIC on new Master FPC going offline. *Resolved In:* junos:21.4R3-S7 junos:22.3R3-S3 junos:22.4R3-S2 junos:23.2R2 junos:23.4R2 junos:24.1R1
PR Number	**Synopsis**	**Category: QFX VC Datapath**
1785882	JDI-RCT : IPCLOS:Azurite:Partial continuos traffic drop observed on ipv4 and ipv6 streams (framing errors) Product-Group=junos Severity=Critical	With SR4 optics on QFX5210 some times we can see Partial continuous traffic drop observed on ipv4 and ipv6 streams (framing errors) *Resolved In:*
PR Number	**Synopsis**	**Category: SRX Gen-3 RE, leveraged from Point Success Mt.Rainier**
1774760	RE switchover observed in SRX5K platforms when ethernet switchports failure scenario on SCB Product-Group=junos Severity=Major	On SRX5K platforms when all ethernet switch ports on Switch Control Board(SCB) fail, it triggers the Routing Engine (RE) switch over and RE0 is stuck in "Disabled" state. As RE0 is disabled and RE1 does have the functionality to coordinate chassis. No PIC will turn up which were failed and triggered the failover and traffic impact will be there for those particular ports and the complete service impact will be there if RE1 had any issue when RE0 is in disable state. RE0 did not recover by its own from the disabled state until manual reboot is done. *Resolved In:* junos:19.4R3-S13 junos:20.2R3-S9 junos:20.4R3-S10 junos:21.2R3-S8 junos:21.4R3-S6 junos:22.1R3-S5 junos:22.2R3-S4 junos:22.3R3-S2 junos:22.4R3-S1 junos:23.2R2 junos:23.4R1 junos:23.4R2 junos:24.1R1
PR Number	**Synopsis**	**Category: SPC3 HW and SW Issues**
1780282	Unexpected failover will be seen when there is communication loss between CP and SPU on SRX platforms with web-authentication or web-redirect is configured Product-Group=junos	On all SRX series firewall with web-authentication or web-redirect configured, with continuous traffic from different IPs for which authentication needs to be done in such scenarios firewall authentication entries are out of sync between Central Point (CP) and Services Processing Units (SPU) modules caused attempt to delete same firewall authentication entry twice, that causes invalid memory access resulting

	Severity=Major	into the core-dump followed by failover. Traffic impact will be seen during the fail over. *Resolved In:* junos:21.2R3-S7 junos:22.3R3-S3 junos:22.4R3-S2 junos:23.2R2 junos:23.4R2 junos:24.1R1
PR Number	**Synopsis**	**Category: "agentd" software daemon**
1647568	SDN-Telemetry process crash during longevity tests of Streaming telemetry. Product-Group=junos Severity=Major	On all Junos platforms, agentd process crash will be seen in telemetry streaming longevity test. *Resolved In:*
1765344	The telemetry stops streaming data when the jsd CPU utilization goes high Product-Group=junos Severity=Minor	On Junos and Junos Evolved platforms, when it enables telemetry and uses the gRPC dial-out method, jsd might be stuck with high CPU utilization, and stop streaming data. *Resolved In:* evo:22.3X50-EVO evo:22.3X80-D43-EVO evo:22.3X80-D44-EVO evo:22.4R2-S1-J1-EVO evo:22.4R3-S1-EVO evo:23.2R2-EVO evo:23.4R1-S1-EVO evo:23.4R2-EVO evo:24.1R1-EVO junos:22.4R3 junos:22.4R3-S1 junos:23.2R2 junos:23.2R2-J14 junos:23.4R1-S1 junos:23.4R2 junos:24.1R1
PR Number	**Synopsis**	**Category: MPC10/11/LC9600 Chassis Category**
1752654	Voltage Threshold Crossed message observed on all Junos OS Evolved platforms Product-Group=junos Severity=Major	On all Junos OS Evolved platforms and device with MX10K-LC2301/ MX10K-LC9600, MX304, LC480, LC2101, LC1201 the voltage threshold cross is reported by MX20796 sensor. *Resolved In:* junos:22.4R3
PR Number	**Synopsis**	**Category: MPC Fusion SW**
1746643	FPC process crash will be observed after performing the ISSU Product-Group=junos Severity=Major	On Junos MX platforms with MPC2E-3D-NG, MPC3E-3D-NG and MPC2E NG HQoS line cards with MIC -> 10x 1GE(LAN) -E SFP, the Flexible PIC Concentrators (FPCs) process crash will be observed after performing the In-Service Software Upgrade (ISSU). *Resolved In:* evo:23.4R1-EVO junos:21.2R3-S5-J12 junos:21.2R3-S7 junos:21.4R3-S6 junos:22.1R3-S5 junos:22.2R3-S4 junos:22.3R3-S2 junos:22.4R3-S2 junos:23.2R2 junos:23.4R1
PR Number	**Synopsis**	**Category: SRX2000/50000 issue**
1663839	Syslog message CHASSISD_IPC_WRITE_ERR_NULL_ARGS are observed at commit Product-Group=junos Severity=Major	Syslog message CHASSISD_IPC_WRITE_ERR_NULL_ARGS is observed at commit on SRX5K platforms. This is caused by unsupported chassis component connection on SRX5K platforms during commit checks. This syslog message is informational only for SRX5K, and was removed. *Resolved In:* junos:20.2R3-S9 junos:20.4R3-S10 junos:21.2R3-S8 junos:21.4R3-S6 junos:22.1R3-S5 junos:22.2R3-S4 junos:22.3R3-S2 junos:22.4R3-S2 junos:23.1R1
1775880	A flowd crash is observed if CP receives the packets due to some hardware memory issue Product-Group=junos Severity=Major	On SRX5K platforms with SPC3 and SPC2 cards, flowd crash will be observed if CP (Central Point) receives the packets due to some hardware memory issue either on IOC (I/O card) or SPC (Services Processing Card) which requires session lookup. *Resolved In:* junos:20.2R3-S9 junos:20.4R3-S10 junos:21.2R3-S8 junos:21.4R3-S6 junos:22.1R3-S5 junos:22.2R3-S4 junos:22.3R3-S2 junos:22.4R3-S1 junos:23.2R2 junos:23.4R1 junos:23.4R2 junos:24.1R1
PR Number	**Synopsis**	**Category: BBE Layer-2 Bitstream Access**
1796125	The broadband subscriber (L2BSA subscribers) on the core interface logging out with interface state	On all Junos platforms, any configuration changes that involve interface down/up sequence, result in logging-out L2BSA (Layer 2 Broadband Subscriber Access)

	changes Product-Group=junos Severity=Major	subscribers associated with that core interface. *Resolved In:* evo:23.4R2-EVO evo:24.1R2-EVO evo:24.2R1-EVO evo:24.3R1-EVO junos:21.2R3-S5-J3 junos:21.2R3-S8 junos:22.1R3-S6 junos:22.2R3-S4 junos:22.3R3-S3 junos:22.4R3-S2 junos:23.2R2-S1 junos:23.4R2 junos:24.1R2 junos:24.2R1 junos:24.3R1
PR Number	**Synopsis**	**Category: BBE routing**
1781938	Access route may get stuck in the routing table after trying to change the prefix length using CoA message Product-Group=junos Severity=Major	On Junos MX platforms with subscribers management enabled, the access route may get stuck in the routing table failing to update or be removed as expected. This occurs when a user attempts to modify the prefix length associated with this route using a Change of Authorization (CoA) message. This may lead to traffic loss, and if a subscriber goes down following the CoA change, there is a failure to bring that specific subscriber back up. *Resolved In:* evo:23.4R2-EVO evo:24.1R1-EVO junos:21.2R3-S5-J32 junos:21.2R3-S8 junos:21.4R3-S7 junos:22.1R3-S5 junos:22.2R3-S4 junos:22.3R3-S3 junos:22.4R3-S2 junos:23.2R2 junos:23.4R2 junos:24.1R1
PR Number	**Synopsis**	**Category: Border Gateway Protocol**
1663883	Traffic loss will be seen due to delay in BGP convergence time Product-Group=junos Severity=Major	On all Junos and Junos Evolved platforms, whenever there is high percentage of background CPU usage that causes the rpd process to run at an average CPU load, BGP convergence will be slow, which results in traffic loss. *Resolved In:* evo:21.4X1-EVO evo:22.3R2-EVO evo:22.3R3-EVO evo:22.3X80-D33-EVO evo:22.4R1-EVO evo:23.4R1-EVO junos:18.2X75-D67 junos:20.3X75-D50 junos:22.3R2 junos:22.3R3 junos:22.4R1 junos:23.4R2 junos:24.1R1
1715771	MD5 password change doesn't put BGP session down Product-Group=junos Severity=Major	For all Junos platforms, authentication for BGP (Border Gateway Protocol) works by adding configured authentication parameters to a file and a module loads that information into kernel for using on both send side and BGP listen socket. As part of this information sent, BGP needs to add which routing-instance table it wants to use to reach the peer. Usually, peers use the routing-tables they are configured in. But when forwarding-context knob in a routing-instance of type no-forwarding is set to master peer will use master's forwarding table for creating the socket and connection. Here the issue customer wants to have same peering addresses in different routing-instances but use the same forwarding-table for peering. For this reason, it is required for them to have same authentication parameters for both the connections. *Resolved In:*
1781859	The rpd process will crash in an EVPN scenario Product-Group=junos Severity=Critical	On all Junos and Junos Evolved platforms, when EVPN-Type 5 (Ethernet VPN-Type 5) and L3VPN (Layer 3 VPN) families are configured and if EVPN routes are advertised to BGP(Internal Border Gateway Protocol) inet-VPN sessions then rpd process crashes. During the rpd crash and restart, the routing protocols will be impacted and traffic disruption will be seen due to the loss of routing information. *Resolved In:* evo:22.3R3-S3-EVO evo:22.4R3-EVO evo:23.2R2-EVO evo:23.4R2-EVO evo:24.1R1-EVO junos:21.4R3-S7 junos:21.4R3-S9 junos:22.1R3-S6 junos:22.2R3-S4 junos:22.3R3-S3 junos:22.4R3 junos:22.4R3-S1 junos:23.2R2 junos:23.2R2-J14 junos:23.4R1-S1 junos:23.4R2 junos:24.1R1
PR Number	**Synopsis**	**Category: Track PRs in BGP BMP area & is part of BGP inside RPD.**
1635143	The rpd may crash due to memory pressure for high BGP scale with flapping route and BGP Monitoring Protocol (BMP) collector/station is very slow on all Junos and EVO platforms Product-Group=junos Severity=Major	On all devices running Junos OS or Junos OS Evolved, where this is a high BGP scale with flapping route and the BGP Monitoring Protocol (BMP) collector/station is very slow, the rpd process might crash due to memory pressure. *Resolved In:* junos:20.3X75-D45
PR Number	**Synopsis**	**Category: BBE Remote Access Server**

1779221	Junos OS Evolved: ACX7000 Series: Ports which have been inadvertently exposed can be reached over the network (CVE-2024-39537) Product-Group=junos Severity=Major	An Improper Restriction of Communication Channel to Intended Endpoints vulnerability in Juniper Networks Junos OS Evolved on ACX7000 Series allows an unauthenticated, network-based attacker to cause a limited information disclosure and availability impact to the device. Please refer to https://supportportal.juniper.net/JSA82997 for more information. *Resolved In:* evo:21.4R3-S7-EVO evo:22.2R3-S4-EVO evo:22.3R3-S3-EVO evo:22.4R3-S2-EVO evo:23.2R2-EVO evo:23.4R1-S1-EVO evo:23.4R2-EVO evo:24.1R1-EVO evo:24.2R1-EVO junos:21.4R3-S7 junos:22.1R3-S6 junos:22.2R3-S4 junos:22.3R3-S3 junos:22.4R3-S2 junos:23.2R2 junos:23.2R2-J14 junos:23.4R1-S1 junos:23.4R2 junos:24.2R1
PR Number	**Synopsis**	**Category: MX304 Chassis specific platform**
1747957	Traces on Line-cards are not available Product-Group=junos Severity=Major	Traces on line cards with no SSDs are not available on line cards as well as RE. There is no infra to transport the traces to RE. *Resolved In:*
1791839	JDI-REGRESSION:MX304: core-spmbpfe-bugatti-pvl-b1 seen in re1 Product-Group=junos Severity=Major	MX304: core-spmbpfe-bugatti-pvl-b1 seen in re1 *Resolved In:*
PR Number	**Synopsis**	**Category: MX304 interface specific**
1752831	Port et-0/0/4 and xe-0/0/5:0 can not be up at the same when port 4 is configured as 100g and port 5 is configured as 1x10G on MX304 Product-Group=junos Severity=Major	Port et-0/0/4 and xe-0/0/5:0 can not be up at the same when port 4 is configured as 100g and port 5 is configurd as 1x10G on MX304. *Resolved In:* evo:23.2R2-EVO evo:23.4R1-EVO junos:22.4R3 junos:23.2R1-S1 junos:23.2R2 junos:23.3R1 junos:23.4R1
PR Number	**Synopsis**	**Category: MX304 line card platform software**
1719483	FPC PLL Input Failure observed on newly booted MX304 boxes Product-Group=junos Severity=Major	On MX304, for releases prior to timing feature support, the internal dpll used for timing is configured with default values which are not valid. Hence the PLL failure alarm might be observed which can be safely ignored *Resolved In:* evo:22.4R3-EVO junos:22.4R1-S2 junos:22.4R3
PR Number	**Synopsis**	**Category: MPC5/6E PFE QOS & HQOS software**
1155610	WRED drops are seen on under subscribed queue when drop-profile-map is not configured Product-Group=junos Severity=Critical	JUNOS software configures default WRED profile when drop-profile-map is not configured in the scheduler associated with a queue. The default WRED profile is configured with (0% fill-level, 0% drop) and (100% fill-level, 100% drop). Under certain traffic conditions, this may result in small percentage of WRED drops even when a queue is under subscribed (fill-level is < 100%). *Resolved In:* junos:14.1R8 junos:14.2R7 junos:15.1F2-S5 junos:15.1F5 junos:15.1F6 junos:15.1R4 junos:16.1R1 junos:16.2R1
PR Number	**Synopsis**	**Category: MX Platform SW - FRU Management**
1681716	The device goes down when an FRU has over-temperature Product-Group=junos Severity=Major	On MX240, MX480, and MX960, when the temperature for a particular FRU is above the over-temperature condition, the chassisd will start the timer(240 secs). If the over-temperature condition persists after completing 240secs, the chassis will be shut down instead of bringing down the particular FRU. This will impact the whole device traffic. *Resolved In:*
PR Number	**Synopsis**	**Category: MX Platform SW - Mastership Module**

1739702	'CHASSISD_IPC_FLUSH_ERROR' is seen on MX platforms after RE upgrade/downgrade having GRES configured Product-Group=junos Severity=Major	On all MX platforms, after the mastership switch over triggered by RE firmware upgrade/downgrade, CHASSID_IPC_FLUSH_ERRORs might be seen as chassisd will be unable to write to the line card pipe due to pfe restart. After a read failure chassisd will shut down the pipe connection, further the error messages will not be seen. PFE restart is expected as this involves an image upgrade. These errors don't have a functional impact. *Resolved In:*
PR Number	**Synopsis**	**Category: QFX Control Plane VXLAN**
1777635	Traffic loss for few seconds will be observed after restarting l2-learning process on L3 VxLAN gateway Product-Group=junos Severity=Major	On all Junos and Junos Evolved platforms, in the EVPN-VXLAN(Ethernet Virtual Private Network- Virtual Extensible Local Area Network) scenario, traffic loss for few seconds would be observed when a user restart l2-learning process on a Layer-3 VXLAN gateway. This happens because of timing issues in the kernel, which mistakenly delete MAC routes of its associated devices instead of updating them in the table. The traffic from devices with those MAC addresses won't flow until the system is back on track and syncing properly. *Resolved In:* evo:22.2R3-S4-EVO evo:22.3R3-S3-EVO evo:22.4R3-S2-EVO evo:23.2R2-EVO evo:23.4R2-EVO evo:24.1R1-EVO junos:22.2R3-S4 junos:22.3R3-S3 junos:22.4R3-S2 junos:23.2R2 junos:23.2R2-J14 junos:23.4R2 junos:24.1R1
PR Number	**Synopsis**	**Category: Platform PR for 1G/10G LC**
1700909	FPC crash is observed and the device is rebooted when multiple interface operations are performed in MX platforms with LC480 linecard Product-Group=junos Severity=Major	On all MX platforms with LC480 linecard, in a rare occurrence, while triggering interface operations on the LC480 linecard, then FPC (Flexible PIC concentrator) crash is observed and the device gets rebooted. *Resolved In:* evo:22.4R2-EVO evo:22.4R3-EVO evo:23.1R1-EVO evo:23.1R2-EVO evo:23.2R1-EVO evo:23.3R1-EVO junos:22.4R2 junos:22.4R3 junos:23.1R1 junos:23.1R2 junos:23.2R1 junos:23.3R1
PR Number	**Synopsis**	**Category: Device Configuration Daemon**
1725168	Traffic impact will be seen with mismatched speeds on the LAG interface and member interface Product-Group=junos Severity=Major	On all Junos platforms, if a speed mismatch happens in the LAG (Link Aggregation) & member interface then a traffic drop will be seen. *Resolved In:* junos:22.2R3-S4 junos:22.4R3-S1 junos:23.2R2 junos:23.4R1
PR Number	**Synopsis**	**Category: CoS support on DNX**
1770491	Traffic convergence is longer than usual after the CoS rewrite Product-Group=junos Severity=Critical	On ACX5448 and ACX710 platforms, traffic convergence takes more time than the expected 50ms i.e. traffic loss is more than expected observed for CoS (Class-of-service) rewrite change after a link failover in the MPLS (Multiprotocol Label Switching) scenario with FRR (Fast Reroute) and LSP (Label-Switched Path) link-protection configured. *Resolved In:* junos:21.4R3-S6 junos:22.3R3-S3 junos:22.4R3 junos:22.4R3-S2 junos:23.2R2 junos:23.4R1-S1 junos:23.4R2 junos:24.1R1
PR Number	**Synopsis**	**Category: EVPN ELAN/E-TREE**
1732448	JDI-RCT:ACX : Syslog error @Err] dnx_rt_vswitch_cross_connect_add_del: dnx_rt_vswitch_cross_connect_add_del:cross-connect delete failed for IFL 135(UNI 1149255708, NNI 402657548) (-1:Internal error) and several related syslog errors after loading configs. Product-Group=junos Severity=Major	JDI-RCT:ACX : Syslog error @Err] dnx_rt_vswitch_cross_connect_add_del: dnx_rt_vswitch_cross_connect_add_del:cross-connect delete failed for IFL 135(UNI 1149255708, NNI 402657548) (-1:Internal *Resolved In:*
PR Number	**Synopsis**	**Category: DNX VPLS**

1692400	dc-pfe: HEAP malloc(0) detected! when a VPLS instance is deactivated in ACX5048. Product-Group=junos Severity=Major	dc-pfe: HEAP malloc(0) detected! when a VPLS instance is deactivated in ACX5048. This are informational messages and the fix of this PR hides the messages from console output. *Resolved In:* junos:20.4R3-S6 junos:21.2R3-S7 junos:22.1R3-S5 junos:22.3R3-S3 junos:22.4R3 junos:23.1R2 junos:23.2R2 junos:23.3R1 junos:23.4R1
PR Number	**Synopsis**	**Category: EVO L2 Control Plane PRs**
1769086	Data center interconnect configuration addition needs to be non-catastrophic. Product-Group=junos Severity=Major	Adding interconnect configuration can be catastrophic behaviour which means BD (Bridge domain) and routing instance object will be deleted and added back, during this window there will be traffic drop. *Resolved In:* evo:21.4R3-S6-EVO evo:22.2R3-S3-EVO evo:22.4R3-EVO evo:22.4R3-S1-EVO evo:23.2R2-EVO evo:23.4R2-EVO evo:24.1R1-EVO junos:21.4R3-S6 junos:21.4R3-S7 junos:22.2R3-S4 junos:22.3R3-S2 junos:22.4R3 junos:22.4R3-S1 junos:22.4R3-S2 junos:23.2R2 junos:23.2R2-J14 junos:23.4R2 junos:24.1R1
PR Number	**Synopsis**	**Category: EVO MACSEC Platform Independent Implementation**
1712554	The MACsec on the channelized IFD impacts the MACsec traffic on other channelized IFL interfaces within the same port and vice versa Product-Group=junos Severity=Major	If both MACsec(media access control security) IFL(interface logical) and MACsec IFD(physical interface device) coexist on the channelized interface, enabling MACsec on the channelized IFD impacts the MACsec traffic on other channelized IFL interfaces within the same port and vice versa. This issue is applicable to MPC10E and MPC11E platforms. *Resolved In:* evo:22.4R2-EVO evo:22.4R3-EVO evo:23.1R2-EVO evo:23.2R1-EVO evo:23.3R1-EVO junos:22.1R3-S3 junos:22.3R3 junos:22.4R3 junos:23.1R2 junos:23.2R1 junos:23.3R1
PR Number	**Synopsis**	**Category: Paragon Active Assurance**
1728816	Junos OS Evolved ACX Series with Paragon Active Assurance Test Agent: A local high privileged attacker can recover other administrators credentials (CVE-2024-30406) Product-Group=junos Severity=Critical	A Cleartext Storage in a File on Disk vulnerability in Juniper Networks Junos OS Evolved ACX Series devices using the Paragon Active Assurance Test Agent software installed on network devices allows a local, authenticated attacker with high privileges to read all other users login credentials. Please refer to https://supportportal.juniper.net/JSA79104 for more information. *Resolved In:* evo:23.2R2-EVO evo:23.3R1-EVO evo:23.3R2-EVO evo:23.4R1-EVO
PR Number	**Synopsis**	**Category: Express ptx-evo PFE L3 Features**
1756452	FPC unreachable due to running out of Guid space Product-Group=junos Severity=Major	FPC unreachable due to running out of Guid space and any stats pooling makes Guid space run out faster. *Resolved In:* evo:22.2R3-S3-EVO evo:22.3X50-EVO evo:22.3X80-D43-EVO evo:22.3X80-D44-EVO evo:22.4R3-EVO evo:22.4R3-S1-EVO evo:23.2R2-EVO evo:23.4R1-EVO evo:23.4R2-EVO evo:24.1R1-EVO junos:23.4R2 junos:24.1R1
PR Number	**Synopsis**	**Category: EVPN control plane issues**
1706682	Traffic loss seen with Multiple IFLs on an IFD with ESI per IFD configuration when one of the IFL disable Product-Group=junos Severity=Critical	If one of the IFL goes down from multiple IFLs on IFD with per ESI configuration, the DF election is triggered and a potential DF switchover happens, This will create some traffic loss for rest of IFL on that ESI. Solution: * Enable the this"set protocols evpn advertise-evpn-esi-routes" knob on all the evpn peer device on before the IFL disable. This is a code modification and not a software bug. *Resolved In:* evo:22.4R3-EVO evo:23.2R2-EVO evo:23.3R2-EVO evo:23.4R1-EVO evo:24.1R1-EVO evo:24.2R2-EVO junos:22.4R3 junos:23.2R2 junos:23.2R2-J14 junos:23.3R2 junos:23.4R1 junos:24.1R1
PR Number	**Synopsis**	**Category: EVPN Layer-2 Forwarding**

1743529	ARP/FIB are added even if IRB in EVPN is disabled Product-Group=junos Severity=Major	On all Junos and Junos Evolved platforms, address resolution protocol (ARP) entry is added via evpn even if the corresponding integrated routing and bridging (IRB) is disabled. Even though an alternative path exists via other interface, the path will not be used and the packet will be dropped. *Resolved In:* evo:22.4R3-EVO evo:23.2R2-EVO evo:23.3R1-EVO evo:23.4R1-EVO junos:22.4R3 junos:23.2R2 junos:23.3R1 junos:23.4R1
PR Number	**Synopsis**	**Category: EX4100 RE, Platform Infra, Drivers**
1756750	Interface on the server side activates during switch boot-up process on EX4100 platforms Product-Group=junos Severity=Minor	On Junos EX4100 platforms, interface on the server side activates during switch boot-up process . *Resolved In:* junos:22.3R3-S2 junos:22.4R2-S2-J1 junos:22.4R3 junos:22.4R3-S1 junos:23.2R2 junos:23.3R2 junos:23.4R1 junos:24.1R1
PR Number	**Synopsis**	**Category: EX interfaces issues**
1580560	On EX2300, EX3400, :EX4300-48MP and EX4300 , Pause frames counters does not get incremented when pause frames are sent. Product-Group=junos Severity=Major	On EX2300, EX3400, :EX4300-48MP and EX4300 , Pause frames counters does not get incremented when pause frames are sent. *Resolved In:*
1749391	[interface] [all] EX4400-48F :: JUNOS_REG: EX4400 : input-vlan-tagged-frames are not in the expected range while verifying Vlan Tagged Frames Product-Group=junosvae Severity=Major	[interface] [all] EX4400-48F :: JUNOS_REG: EX4400 : input-vlan-tagged-frames are not in the expected range while verifying Vlan Tagged Frames *Resolved In:*
1789999	[interfaces]:Ex-Hardening:Local/Remote fault insertion from TG is failing Product-Group=junos Severity=Major	Ex-Hardening:Local/Remote fault insertion from TG is failing *Resolved In:*
PR Number	**Synopsis**	**Category: EX4400 PFE software**
1752171	MIST JVD:: EX4400-VC:: BGP Adjacency flap observed on VC Mastership switchover by rebooting present Master Product-Group=junos Severity=Major	In the transition to the master switchover in EX, the current 350 ms duration for the underlay session timer is deemed too aggressive. To ensure a smoother and more reliable switchover process, it is recommended to extend the timer. This adjustment will provide additional time for the underlay session to stabilize and reduce the potential for disruptions or inconsistencies during the master switchover. *Resolved In:*
PR Number	**Synopsis**	**Category: EX4400 platform**
1709431	MACsec:Traffic loss is seen while testing macsec scale. Product-Group=junos Severity=Major	When high number of MACsec sessions present (more than 200) and traffic is passed over these interface, some of the MACsec session flap and there is traffic drop. *Resolved In:*
PR Number	**Synopsis**	**Category: Express PFE FW Features**
1740257	The inetflow6 routes are not installed on firewall filter table using BGP FlowSpec Product-Group=junos Severity=Major	On all Junos and Junos OS Evolved platforms configured with BGP FlowSpec, ipv6 routes are installed in flow route table but not in firewall filter table. FlowSpec routes are blocked and dropped leading to traffic disruption. This is especially seen when BGP UPDATE Message does not include "Filter: Packet Length filter" within "FLOW_SPEC_NLRI" from BGP flowspec server thereby inetflow6 routes do not have "Action(s)" *Resolved In:* evo:21.4X9-EVO evo:22.2R3-S4-EVO evo:22.3R3-S3-EVO evo:22.4R3-S2-EVO evo:23.2R2-EVO evo:23.3R1-EVO evo:23.4R1-EVO evo:23.4R2-S2-EVO

		junos:21.4R3-S7 junos:22.1R3-S6 junos:22.2R3-S4 junos:22.4R3-S2 junos:23.2R2 junos:23.2R2-J14 junos:23.3R1 junos:23.4R1
PR Number	**Synopsis**	**Category: Express PFE L2 fwding Features**
1792128	Configuring multiple IFL of different families on Junos QFX10K SP style interfaces leads to traffic loss Product-Group=junos Severity=Major	On Junos QFX 10K platforms, traffic drop is seen when multiple interface logical (IFLs) of different families are configured on the same interface physical (IFD) with Service Provide (SP) style configuration and layer 2 (L2) ILF is the first IFL to be created. *Resolved In:* evo:24.2R2-EVO evo:24.3R1-EVO junos:22.2R3-S4 junos:22.4R3-S3 junos:23.4R2 junos:24.2R1 junos:24.2R2 junos:24.3R1
1793335	Nexthop resolution will fail in high scale ARP on QFX10K Platforms Product-Group=junos Severity=Major	On QFX10K platforms, at high scale Address Resolution Protocol (ARP) which is more than 90K that includes ARP learnt on local interfaces and learnt from remote Provider Edges(PEs) on the device in that situation if there is a network event in place such as Flap in access ports or Flap in Datacenter Interconnect links or following network operational commands "clear bgp neighbors" or "restart routing" or "clear ethernet-switching table" or "clear ethernet-switching mac-ip-table" are executed in the device which will create a problem in nexthop token allocation as system reaches maximum token limit. This results a traffic impact for ongoing and upcoming traffic flows. *Resolved In:* junos:22.2R3-S4 junos:23.4R2 junos:24.2R1 junos:24.3R1
1793772	L3 multicast traffic gets dropped when a BD is configured with IRB as the source interface Product-Group=junos Severity=Major	On QFX10002-60C, when Bridge Domain (BD) is configured with Integrated Routing and Bridging (IRB) interfaces acting as ingress for Layer 3 multicast traffic and BD is not a part of Virtual Extensible Local Area Network (VXLAN), then Layer 3 multicast traffic is dropped. *Resolved In:* junos:23.4R2 junos:24.2R2 junos:24.3R1 junos:24.4R1
PR Number	**Synopsis**	**Category: Express PFE L3 Multicast**
1774562	PIM join are not learnt for multicast IPs Product-Group=junos Severity=Critical	On Junos PTX platforms, with PIM BIDR (Protocol Independent Multicast-Bidirectional) mode with "set protocols pim rp bidirectional address <> group-ranges <>" configuration, PIM/MLD joins will not be learnt for multicast IPs other than link local IP and MY IP which will lead to traffic impact. Also, lo0 filter which were introduced with PR 1701756 for IGMP and MLD will be applied only for MY IPs and Link local IPs. For any other IPs other than above, lo0 filter will not work. *Resolved In:* junos:20.3X75-D440 junos:20.3X75-D52 junos:21.2R3-S8 junos:21.4R3-S7 junos:22.1R3-S6 junos:22.2R3-S4 junos:22.3R3-S3 junos:22.4R3-S1 junos:22.4R3-S2 junos:23.2R2 junos:23.4R1-S1 junos:23.4R2 junos:24.1R1
PR Number	**Synopsis**	**Category: SRX1500 platform software**
1751496	On SRX1500 PEM Alarms are displayed due to hardware limitations to read I2C Product-Group=junosvae Severity=Major	On SRX1500 Hardware Limitation leads to PEM I2C Failure Alarm triggered as result of failure in I2C reading operations. *Resolved In:* junos:21.4R3-S7 junos:22.1R3-S6 junos:22.2R3-S4 junos:22.3R3-S3 junos:22.4R3-S1 junos:23.2R2 junos:23.4R1-S2 junos:23.4R2 junos:24.1R1 junos:24.2R1
PR Number	**Synopsis**	**Category: ACX7332 & ACX7348 Platform Software**
1758601	Wrong SNMP jnxOperatingTemp value in negative temperature Product-Group=junos Severity=Major	SNMP jnxOperatingTemp OID shows wrong value during negative temperature, in other temperature range it shows correct value. *Resolved In:* evo:23.2R2-EVO evo:23.4R1-EVO evo:24.1R1-EVO junos:22.4R3 junos:23.2R2 junos:23.2R2-J14 junos:23.4R1 junos:24.1R1
PR Number	**Synopsis**	**Category: SRX4100/SRX4200 platform software**

1689990	Minor alarm "FPC Inefficient Port Mapping" won't be cleared Product-Group=junos Severity=Major	In SRX4100/4200 platform, even assigning ports are balanced, minor alarm "FPC Inefficient Port Mapping" might not be cleared. *Resolved In:* junos:20.4R3-S10 junos:21.2R3-S4 junos:21.3R3-S3 junos:21.4R3-S4 junos:22.1R3 junos:22.1R3-S3 junos:22.2R3 junos:22.3R2 junos:22.3R2-S1 junos:22.4R1 junos:23.1R1
PR Number	**Synopsis**	**Category: Libjtask for RPD tasks, scheduler, timers, memory, and slip**
1787707	The KRT queue will be stuck on Junos ACX710 platform Product-Group=junos Severity=Major	On Junos ACX710 platform with BGP (Border Gateway Protocol) configuration, the response message will be lost and it will lead to element being stuck in the KRT (Kernel Routing Table) queue. *Resolved In:* evo:23.4R2-EVO junos:21.2R3-S8 junos:22.4R3-S2 junos:23.4R2
PR Number	**Synopsis**	**Category: Kernel software for AE/AS/Container**
1747289	VRRP traffic will drop when the member link from the AE bundle is deleted, even if there are active members in the AE bundle Product-Group=junos Severity=Major	On Junos using afeb/tfeb way of communication to PFE that is MX80/MX104 platforms with Virtual Router Redundancy Protocol (VRRP) configured, deleting a member link from the Aggregated Ethernet (AE) bundle removes the VRRP filter entry in the Packet Forwarding Engine (PFE) which causes VRRP traffic to get dropped even though other active member links in the AE bundle exists. *Resolved In:* junos:20.4R3-S9 junos:21.2R3-S8 junos:22.4R3 junos:23.4R2 junos:24.1R1
PR Number	**Synopsis**	**Category: ISIS routing protocol**
1667575	When the SPF algorithm for IS-IS in Segment Routing use case is triggered frequently, CPU usage might increase Product-Group=junos Severity=Major	On all Junos and Junos Evolved platforms, when the shortest-path-first (SPF) algorithm for IS-IS is triggered frequently, CPU usage might increase and impact the device performance and traffic. *Resolved In:* evo:22.4R1-EVO junos:22.4R1
1723172	The rpd process crash is observed when TI-LFA feature is enabled Product-Group=junos Severity=Major	On all Junos and Junos Evolved platforms with TI-LFA (Topology-Independent Loop-Free Alternate) feature enabled, when IP address is removed from one interface and is assigned to another interface in the same commit, the rpd process crashes affecting routing control plane. *Resolved In:* evo:22.4R3-EVO evo:23.2R2-EVO evo:23.3R1-EVO junos:22.4R3 junos:22.4R3-S1 junos:23.2R2 junos:23.3R1
1746557	Stale IP prefixes when issuing "show isis route flex-algorithm-id" Product-Group=junos Severity=Minor	The Flex algorithm in IS-IS does not install IP (v4/v6) routes into the RIB. However, when using the current IS-IS show CLI command, "show isis route flex-algorithm-id <>", it still displays certain IPv4/IPv6 IS-IS routes in the output, even though these routes are not actually being placed in the RIB. After implementing the fix, the IPv4/IPv6 IS-IS routes will no longer be displayed in the output of the CLI for the flex-algorithm. *Resolved In:* evo:22.2R3-S4-EVO evo:22.4R3-EVO evo:23.1R2-EVO evo:23.2R2-EVO evo:23.3R1-EVO evo:23.4R1-EVO junos:22.2R3-S4 junos:22.4R3 junos:23.1R2 junos:23.2R2 junos:23.3R1 junos:23.4R1
PR Number	**Synopsis**	**Category: jdhcpd daemon**
1775108	DHCP ALQ subscribers may not logged out after TCP connection is removed on all Junos platforms Product-Group=junos Severity=Major	On all Junos platforms with ALQ (Active-Lease Query) enabled with DHCP(Dynamic Host Configuration Protocol) relay agent configuration, with inflight subscribers login & logout and TCP connection reset, the DHCP subscribers may not properly release their IP address leases from a backup DHCP Relay, leading to inaccurate IP address management and allocation for the subscribers. This can lead to traffic impact for subscribers who are not released. *Resolved In:* junos:21.4R3-S6 junos:22.1R3-S5 junos:22.2R3-S4 junos:22.3R3-S3 junos:22.4R3-S2 junos:23.2R2 junos:23.4R2 junos:24.1R1

1778876	DHCP Server in ALQ redundancy: DHCP ACK on renew does not include option 1 subnet mask after failover Product-Group=junos Severity=Major	With DHCP Local Server with Active Lease Query, the DHCP ACK on the DHCP Renew after failover to the back-up server does not provide a response for option 1 subnet mask *Resolved In:* junos:22.3R3-S1-J2 junos:22.3R3-S3 junos:22.4R3-S3 junos:23.2R2 junos:23.4R2 junos:24.1R1
PR Number	**Synopsis**	**Category: Juniper Device Manager VM Mgmt and infrastructure function**
1675919	NFX350 :: JDI_REGRESSION:PLATFORM:SWITCHING:JDM:: Core "localhost.libvirtMib_suba.15909.1656455866.core.tgz" is seen on NFX-350 boxes Product-Group=junos Severity=Critical	NFX350 :: JDI_REGRESSION:PLATFORM:SWITCHING:JDM:: Core "localhost.libvirtMib_suba.15909.1656455866.core.tgz" is seen on NFX-350 boxes *Resolved In:*
PR Number	**Synopsis**	**Category: Firewall Authentication**
1732210	23.1R2:ISSU:USERFW-CP: Clearpass Auth entry's are getting deleted post successful ISSU Product-Group=junos Severity=Major	On SRX devices on aruba-clearpass webapi configuration set system services webapi <*> authentication entries could be lost during ISSU or during Junos version upgrades to 23.1 from prior versions. Due to this issue any dataplane traffic using the ClearPass Authentication entries will require reauthentication. *Resolved In:* junos:23.4R2 junos:24.1R1
PR Number	**Synopsis**	**Category: Flow Module**
1761542	In a chassis cluster setup the flowd crashes and SPC cards will fail Product-Group=junos Severity=Major	On SRX platforms, in a chassis cluster setup configured in Active/Active mode, the fabric forward packet enters the flow module causing the flow processing daemon (flowd) to crash, impacting the traffic forwarding and failing the Services Processing Card (SPC). *Resolved In:* junos:21.4R3-S8 junos:23.4R2 junos:24.2R2 junos:24.3R1
1762568	Unable to download a file completely from SaaS server to LAN Product-Group=junos Severity=Major	TCP sessions are not refreshed when enabled the "set security flow gre-perf-acceleration" is configured. *Resolved In:* junos:22.1R3-S5 junos:22.2R3-S4 junos:22.3R3-S3 junos:22.4R3-S2 junos:23.2R2 junos:23.4R1-S2 junos:23.4R2 junos:24.1R1
1776480	The nsd process goes high on primary device when the Tenant System is configured Product-Group=junos Severity=Major	On SRX 1500, SRX4K , SRX5K series platforms and vSRX, the nsd process will remain high on primary device after the reboot of the device or power outage or RG0 failover (in chassis cluster scenario) if Tenant Systems are configured. This can lead to traffic loss and outages in the network. *Resolved In:* junos:21.4R3-S6 junos:22.1R3-S5 junos:22.3R3-S2 junos:22.4R3-S2 junos:23.2R2 junos:23.4R2 junos:24.1R1
1776940	Junos OS: SRX4600, SRX5000 Series: TCP packets with SYN/FIN or SYN/RST are transferred after enabling no-syn-check with Express Path (CVE-2024-39561) Product-Group=junos Severity=Major	An Improper Check for Unusual or Exceptional Conditions vulnerability in the flow daemon (flowd) of Juniper Networks Junos OS on SRX4600 and SRX5000 Series allows an attacker to send TCP packets with SYN/FIN or SYN/RST flags, bypassing the expected blocking of these packets. Please refer to https://supportportal.juniper.net/JSA83021 for more information. *Resolved In:* junos:19.1R3-S12 junos:19.2R3-S9 junos:19.3R3-S10 junos:19.4R3-S14 junos:20.2R3-S9 junos:21.2R3-S8 junos:21.4R3-S7 junos:22.1R3-S6 junos:22.2R3-S4 junos:22.3R3-S3 junos:22.4R3-S2 junos:23.2R2 junos:23.2R2-S1 junos:23.4R1-S1 junos:23.4R2 junos:24.1R1 junos:24.2R2 junos:24.3R1
1783595	PMI sends packets to the wrong destination Product-Group=junos Severity=Major	On SRX platform, when the next-hop changes, the PowerMode Ipsec (PMI) induces the packets to be sent to the wrong destination, causing packet drops. *Resolved In:* junos:21.2R3-S8 junos:21.4R3-S7 junos:22.1R3-S6 junos:22.2R3-S4 junos:22.3R3-S3 junos:22.4R3-S2 junos:23.2R2 junos:23.4R2 junos:24.1R1 junos:24.2R1

PR Number	Synopsis	Category: High Availability/NSRP/VRRP
1702763	The secure tunnel interface does not work properly in SRX standalone mode Product-Group=junos Severity=Major	On Junos SRX5400/5600/5800/4100/4200/4600/1500/vSRX3.0 platforms, when the secure tunnel interface (st0) st0.16000-st0.16385 is defined in standalone mode, st0.16000-st0.16385 does not work properly which leads to a traffic impact. From 20.4R1 onwards, st0.16000-st0.16385 is hardcoded to be added to a high-availability zone, so it will not work in other zones. *Resolved In:* junos:20.4R3-S7 junos:21.2R3-S8 junos:21.4R3-S3 junos:22.1R3-S5 junos:22.2R3 junos:22.3R2 junos:22.3R3 junos:22.4R2 junos:23.1R1 junos:23.2R1
1726753	Traffic loss after RG1 failover Product-Group=junos Severity=Major	On vSRX3.0, after an Redundancy Group (RG1+) failover, packets may be sent from the SRX physical interface's MAC address instead of the Redundant Ethernet interface (reth's) virtual MAC which can result in traffic loss. *Resolved In:* junos:20.4R3-S10 junos:21.2R3-S8 junos:21.4R3-S6 junos:22.1R3-S5 junos:22.3R3-S2 junos:22.4R3 junos:23.1R2 junos:23.2R1 junos:23.3R1
1736498	In SRX MNHA cluster setup the RSI takes long time to generate Product-Group=junos Severity=Major	In SRX MNHA cluster setup the RSI takes long time to generate on the MNHA backup node. The RSI includes the command "show security flow session session-state warm" which will collect all the sessions in warm state on the MNHA backup node - this output can be extensive and RSI is being generated an extended period of time, in known instances this was 1-2 hours. *Resolved In:* junos:20.2R3-S9 junos:20.4R3-S10 junos:21.2R3-S8 junos:21.4R3-S5 junos:21.4R3-S6 junos:22.1R3-S4 junos:22.1R3-S5 junos:22.1R3-S6 junos:22.2R3-S4 junos:22.3R3 junos:22.3R3-S1 junos:22.3R3-S2 junos:22.3R3-S3 junos:22.4R2-S1 junos:22.4R3 junos:22.4R3-S1 junos:23.1R2 junos:23.2R2 junos:23.3R1 junos:23.4R1
PR Number	**Synopsis**	**Category: Firewall Policy**
PR Number	**Synopsis**	**Category: IPSEC/IKE VPN**
1778122	On SRX1500 platform In-service software upgrade will fail with error "timeout waiting for secondary node node1 to sync(error-code: 6.1)" Product-Group=junos Severity=Major	On SRX1500 platform with chassis cluster, when In-service software upgrade (ISSU) is initiated and the secondary node will be upgraded to target release. However, the SPU synchronization on secondary node will fail resulting in ISSU aborting and primary node will stay non upgraded. The error "timeout waiting for secondary node node1 to sync(error-code: 6.1)" will be reported on console. *Resolved In:* junos:22.2R3-S4
PR Number	**Synopsis**	**Category: Security platform jweb support**
1786296	Junos OS: SRX Series, EX Series: J-Web: An unauthenticated, network-based attacker can perform XPATH injection attack against a device Product-Group=junos Severity=Critical	An Improper Neutralization of Data within XPath Expressions ('XPath Injection') vulnerability in J-Web shipped with Juniper Networks Junos OS allows an unauthenticated, network-based attacker to execute remote commands on the target device. Please refer to https://supportportal.juniper.net/JSA83023 for more information. *Resolved In:* evo:23.4R2-EVO evo:24.1R1-EVO evo:24.2R1-EVO junos:19.3R3-S10 junos:19.4R3-S14 junos:20.2R3-S9 junos:21.2R3-S8 junos:21.4R3-S7 junos:22.1R3-S6 junos:22.2R3-S4 junos:22.3R3-S3 junos:22.4R3-S2 junos:23.2R2 junos:23.2R2-S1 junos:23.4R1-S1 junos:23.4R2 junos:24.1R1 junos:24.2R1
1788364	J-Web default session limits has been aligned with CLI default values Product-Group=junos Severity=Major	If session limit not configured in cli, default value of session limit will be 7 for Seige models and 1024 for other models *Resolved In:* junos:22.1R3-S6 junos:22.3R3-S3 junos:22.4R3-S2 junos:23.4R2 junos:24.1R1 junos:24.2R1
1789466	Jweb does not display address book entries properly after certain operations. Product-Group=junos Severity=Major	On SRX platform, Jweb does not display address book entries properly after certain operations. *Resolved In:* junos:21.4R3-S7 junos:22.2R3-S4 junos:22.4R3-S2 junos:23.2R2-S1 junos:23.4R2 junos:24.1R1 junos:24.2R1

PR Number	Synopsis	Category: Layer 2 Circuit issues
1779240	The rpd process crash will be observed when the revert timer is changed in pseudowires Product-Group=junos Severity=Minor	On Junos and Junos OS Evolved platforms in l2circuit (Layer 2 Circuit), VPWS (Virtual Private Wire Service), or VPLS (Virtual private LAN service) multihomed scenarios, if the revert timer is changed while using the backup path, the rpd process crash will be observed when the path switches back to the primary. This crash will lead to a temporary traffic drop. *Resolved In:* evo:22.3R3-S3-EVO evo:22.4R3-S1-EVO evo:23.2R2-EVO evo:23.4R2-EVO evo:24.1R1-EVO evo:24.2R1-EVO junos:21.4R3-S7 junos:22.1R3-S6 junos:22.2R3-S4 junos:22.3R3-S3 junos:22.4R3-S1 junos:23.2R2 junos:23.2R2-J14 junos:23.4R2 junos:24.1R1 junos:24.2R1
PR Number	**Synopsis**	**Category: Layer 2 Control Module**
1787892	Interface configured with BPDU-disable goes down during VC mastership switchover Product-Group=junos Severity=Major	On Junos EX3400/EX4300/EX2300 platforms configured with VC (Virtual Chassis) and NSB (Nonstop-Bridging) enabled, when VC mastership switchover is triggered, the configuration under 'set protocols layer2-control bpdu-block interface ' will not take effect due to which the interface will go down and will impact the traffic. The configuration 'set protocols layer2-control bpdu-block interface all' will not have any impact. *Resolved In:* evo:22.3R3-S3-EVO evo:23.4R2-EVO evo:24.1R1-EVO evo:24.2R1-EVO junos:21.4R3-S7 junos:22.1R3-S6 junos:22.2R3-S4 junos:22.3R3-S3 junos:22.4R3-S2 junos:23.2R2 junos:23.2R2-S1 junos:23.4R2 junos:24.1R1 junos:24.2R1
PR Number	**Synopsis**	**Category: Layer2 forwarding on EX/NTF/PTX/QFX**
1772424	Connectivity between static and LDP signaled pseudowires broken in VPLS after upgrade and results in VPLS traffic drop Product-Group=junos Severity=Major	On all Junos and Junos OS Evovled platforms, when there is a upgrade and also when one mesh group of routing instance is substring of other, the connection between static and LDP (Label Distribution Protocol) signaled psuedowires is broken will lead to traffic drop. *Resolved In:* evo:21.2R3-S8-EVO evo:21.4R3-S7-EVO evo:22.2R3-S4-EVO evo:22.3R3-S3-EVO evo:22.4R3-S2-EVO evo:23.2R2-EVO evo:23.4R2-EVO evo:24.1R1-EVO evo:24.2R1-EVO junos:21.2R3-S8 junos:21.4R3-S7 junos:22.1R3-S6 junos:22.2R3-S4 junos:22.3R3-S3 junos:22.4R3-S2 junos:23.2R2 junos:23.2R2-J14 junos:23.4R2 junos:24.1R1 junos:24.2R1
1776991	ARP resolution issues will be observed in the H-VPLS environment Product-Group=junos Severity=Major	On Junos and Junos Evolved platforms, traffic impact will be observed due to ARP (Address Resolution Protocol) resolution issues when multiple mesh-group is configured under the same routing-instance and the name of each mesh-group is not unique i.e. substring of another mesh-group in the H-VPLS (Hierarchical Virtual Private LAN Service) environment. *Resolved In:* evo:21.2R3-S8-EVO evo:21.4R3-S7-EVO evo:22.2R3-S4-EVO evo:22.3R3-S3-EVO evo:22.4R3-S1-EVO evo:23.2R2-EVO evo:23.4R2-EVO evo:24.1R1-EVO junos:21.2R3-S8 junos:21.4R3-S6 junos:22.1R3-S5 junos:22.1R3-S6 junos:22.2R3-S4 junos:22.3R3-S3 junos:22.4R3-S1 junos:23.2R2 junos:23.2R2-J14 junos:23.4R2 junos:24.1R1
PR Number	**Synopsis**	**Category: lacp protocol**
1783793	All AEs bundles configured in Active-Standby mode for EVPN-MPLS routing-instances will flap on the first commit post a fresh system reboot Product-Group=junos Severity=Major	On all Junos MX and EX platforms with MPC family of line cards, all the Aggregated-Ethernet (AEs) bundles configured in Active-Standby mode for Ethernet Virtual Private Network-Multiprotocol Label Switching (EVPN-MPLS) routing-instances on the system will flap on the first commit after a fresh system reboot. *Resolved In:* junos:21.4R3-S4-J21 junos:21.4R3-S6 junos:22.1R3-S6 junos:22.2R3-S4 junos:22.3R3-S3 junos:22.4R3-S2 junos:23.2R2 junos:23.4R1-S1 junos:23.4R2 junos:24.1R1 junos:24.2R1
PR Number	**Synopsis**	**Category: Port-based link layer security services and protocols that a**

1729467	MACsec interoperability issue between Juniper and non Juniper platforms Product-Group=junos Severity=Major	On all Junos and Junos Evolved platforms with MACsec (Media Access Control security) configured , frequent SAK (Secure Association Key) rollover is observed when the peer device is a non-Juniper box and the Juniper device is acting as the key-server. This results in unstable MACsec sessions between the juniper device and the non Juniper device. *Resolved In:* evo:22.2R3-S4-EVO evo:22.3R3-S3-EVO evo:22.4R3-S1-EVO evo:23.2R2-EVO evo:23.3R1-EVO junos:20.3X75-D36 junos:20.3X75-D440 junos:21.2R3-S8 junos:21.4R3-S7 junos:22.1R3-S6 junos:22.2R3-S4 junos:22.3R3-S3 junos:22.4R3 junos:22.4R3-S1 junos:23.2R2 junos:23.2R2-J14 junos:23.3R1
PR Number	**Synopsis**	**Category: Multiprotocol Label Switching**
1575060	The LSP might fail to be established when IS-IS-TE or OSPF-TE is enabled Product-Group=junos Severity=Major	If IS-IS-TE or OSPF-TE is enabled, but extended admin groups (which is configured under routing-options) are configured after the peer router advertises the extended admin groups, the LSP with extended admin groups constraints might fail to be established. *Resolved In:* evo:21.3R1-EVO junos:20.3X75-D35 junos:20.3X75-D40 junos:20.4R3-S10 junos:21.3R1
1759082	Junos OS and Junos OS Evolved: Inconsistent information in the TE database can lead to an rpd crash (CVE-2024-39541) Product-Group=junos Severity=Major	An Improper Handling of Exceptional Conditions vulnerability in the Routing Protocol Daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated, adjacent attacker to cause a Denial-of-Service (DoS). Please refer to https://supportportal.juniper.net/JSA83001 for more information. *Resolved In:* evo:22.3X50-EVO evo:22.4R3-S2-EVO evo:23.2R2-EVO evo:23.4R1-S1-EVO evo:23.4R2-EVO evo:24.1R1-EVO junos:22.4R3-S1 junos:22.4R3-S2 junos:23.2R2 junos:23.2R2-J14 junos:23.4R1-S1 junos:23.4R2 junos:24.1R1
1775553	Traffic drop in L2VPN scenarios when an access port flap or configuration change Product-Group=junos Severity=Major	On Junos QFX5100 and EX4600 platforms in Layer 2 Virtual Private Network (L2VPN) scenarios, when an access port flaps or the port related configuration is deactivated and activated, the traffic ingressing or egressing out of that port gets dropped. *Resolved In:* junos:20.4R3-S10 junos:21.4R3-S6
PR Number	**Synopsis**	**Category: Multicast Routing**
1777774	The rpd process crash is observed when MVPN PE receives PIM join messages from the remote peers Product-Group=junos Severity=Major	On all Junos Evolved platforms, when MVPN (Multicast Virtual Private Network) configured device receives PIM join or IGMP report from the remote peer installs route in next-hop and not in multicast composite next-hop, causing the rpd process to crash. *Resolved In:* evo:22.1R3-S5-EVO evo:22.2R3-S3-EVO evo:22.3R3-S2-EVO evo:22.4R3-S1-EVO evo:23.2R2-EVO evo:23.4R2-EVO evo:24.1R1-EVO junos:22.1R3-S5 junos:22.3R3-S2 junos:22.4R3-S1 junos:23.2R2 junos:23.2R2-J14 junos:23.4R2 junos:24.1R1
PR Number	**Synopsis**	**Category: For multicast snooping on MX**
1710565	In a scaled setup mcsnoopd is taking high CPU causing traffic drop Product-Group=junos Severity=Major	On all Junos and Junos Evolved platforms, whenever a commit is done, that involves mcsnoopd daemon config parsing such as (VLAN creation/deletion, interface add/delete to VLAN, interface enable/disable, IGMP (Internet Group Management Protocol) snooping/MLD (Multicast Listener Discovery) snooping related config commands) mcsnoopd will consume CPU. In less scaled setup (few IGMP snooping enabled VLANs and few hundred IGMP snooping memberships), the CPU time taken is less. In a more scaled setup (many IGMP snooping-enabled VLANs and a few thousand IGMP snooping memberships), the CPU may reach >90%. Since mcsnoopd is taking high CPU, it may affect other daemons like rpd. It may affect all the protocols if the CPU is not available to the protocols/daemons. This can impact route entries expiring and cause traffic drop. *Resolved In:* evo:22.2R3-S5-EVO evo:22.3R3-S4-EVO evo:23.2R2-S2-EVO evo:23.4R2-EVO junos:22.3R3-S4 junos:22.4R3-S2 junos:23.2R2-S2 junos:23.4R2 junos:24.1R1

PR Number	Synopsis	Category: Multicast for L3VPNs
1700345	The rpd crash happens when Multicast VPN (Virtual Private Network) is configured with separate route-targets scenario Product-Group=junos Severity=Major	This happens only when MVPN protocol has separate route targets configured and then both the address families are disabled. rpd (Routing process daemon) infra parsing does not check if MVPN protocol is disabled and hence will create the auto policies for route-targets if configured. So if those policies are not marked as active in MVPN configuration flow, it does not get resolved and thereby the policy object may not be valid thus leading to the core. *Resolved In:* evo:22.4R3-EVO evo:23.1R2-EVO evo:23.2R1-EVO junos:22.4R3 junos:23.1R2 junos:23.2R1
PR Number	**Synopsis**	**Category: MX Timing software**
1781161	The external clock is stuck in a Holdover State when an RE switchover is performed Product-Group=junos Severity=Major	On MX platforms, with Graceful Routing Engine Switchover (GRES) enabled and when Routing Engine switchover is performed, the system configured for external synchronization will be stuck in a Holdover State and remain in that state. *Resolved In:* evo:23.4R2-EVO evo:24.1R1-EVO evo:24.2R1-EVO junos:21.2R3-S5-J19 junos:21.2R3-S8 junos:22.1R3-S6 junos:22.3R3-S3 junos:22.4R3-S2 junos:23.2R2 junos:23.4R2 junos:24.2R1
PR Number	**Synopsis**	**Category: Track Mt Rainier RE platform software issues**
1778324	The FPC connection times out and reboots post mastership switchover Product-Group=junos Severity=Major	On Junos MX and PTX with VMHost MT-RE (NG-RE), when the RE< -> CB link down triggers the Routing Engine (RE) switchover, the switchover will be successful but Flexible PIC Concentrators (FPC) will not reconnect to the new master RE. The FPCs reboot and then connect to the new master RE automatically. *Resolved In:* evo:23.4R2-EVO evo:24.1R1-EVO evo:24.2R1-EVO junos:21.2R3-S8 junos:23.2R1-S1-J8 junos:23.2R2-S1 junos:23.4R2 junos:24.1R1 junos:24.2R1
PR Number	**Synopsis**	**Category: Odin Timing software**
1760551	CLKSYNCD_FAULT_NO_MORE_REFERENCE_CLEAR message is logged frequently after deactivating and activating chassis synchronization Product-Group=junos Severity=Major	On all Junos and Junos OS Evolved platforms, when SyncE/PTP is configured, after deactivating and activating chassis synchronization CLKSYNCD_FAULT_NO_MORE_REFERENCE_CLEAR log message is logged every second . *Resolved In:* junos:22.4R3 junos:23.2R2 junos:23.3R2 junos:23.4R1 junos:24.1R1
PR Number	**Synopsis**	**Category: Kernel Multicast Infrastructure**
1740390	vPTX: PFE crash is seen due to invalid token from RPD Product-Group=junos Severity=Major	On vPTX platforms, the PFE (packet forwarding engine) receives an invalid token from RPD (Routing Engine daemon) for composites next-hops due to which the PFE will crash leading to traffic drop. *Resolved In:* junos:21.4R3-S6 junos:22.1R3-S5 junos:22.4R3-S1 junos:23.2R2 junos:23.4R2 junos:24.1R1
PR Number	**Synopsis**	**Category: Kernel Tunnel Interface Infrastructure**
1753191	ARP resolution failure for lt interfaces is observed after cluster failover on Junos SRX platforms Product-Group=junos Severity=Major	On Junos SRX platforms in cluster, Address Resolution Protocol (ARP) resolution fails for logical tunnel interfaces when the logical tunnel interfaces are toggled and the cluster switchovers. *Resolved In:* junos:21.2R3-S8 junos:21.4R3-S7 junos:22.1R3-S6 junos:22.2R3-S4 junos:22.3R3-S3 junos:22.4R3-S2 junos:23.2R2 junos:23.4R2 junos:24.1R1 junos:24.2R1
PR Number	**Synopsis**	**Category: vMX Data Plane Issues**

1669261	vMX crashes due to MBUF leaks Product-Group=junos Severity=Major	vMX platforms (MX150) will crash as a result of the MBUF (Memory Buffer) leak. *Resolved In:* junos:20.3X75-D43 junos:20.3X75-D46 junos:20.4R3-S5 junos:21.4R3 junos:22.1R3 junos:22.3R1 junos:22.3R2 junos:22.3R3 junos:22.4R2 junos:22.4R3 junos:23.1R1
PR Number	**Synopsis**	**Category: Protocol Independant Multicast**
1621358	Initial multicast register packets may get dropped Product-Group=junos Severity=Major	On MX platforms, initial multicast register packets may get dropped, this may affect multicast services. *Resolved In:* evo:20.4R3-S3-EVO junos:19.3R3-S6 junos:19.4R3-S9 junos:20.4R3-S3 junos:21.2R3-S2 junos:22.3R1 junos:23.4R2
1792886	The rpd crash is observed when PIM SSM mode with RPF-Vector and MoFRR is configured Product-Group=junos Severity=Major	On Junos and Junos Evolved platforms , when PIM SSM (PIM Source-Specific Multicast) with RPF (Reverse Path Forwarding)-Vector and MoFRR (Multicast-only fast reroute) is configured , rpd crash if the device receives PIM Prune message for (S, G) state with RPF vector TLV. interface is freed for the (S, G) from the outgoing interface list i.e. RPF-Vector TLV (Type, Length, and Value) having (S, G) is getting freed but that same (S, G) is still used by MoFRR. The issue happens when MoFRR Backup upstream interface is also listed at the outgoing interface list for the (S, G) *Resolved In:* evo:21.2R3-S8-EVO evo:21.4R3-S7-EVO evo:22.2R3-S4-EVO evo:22.3R3-S3-EVO evo:23.2R2-EVO evo:23.4R2-EVO evo:24.1R2-EVO evo:24.2R1-EVO junos:21.2R3-S3-J31 junos:21.2R3-S7-J1 junos:21.2R3-S8 junos:21.4R3-S7 junos:22.1R3-S6 junos:22.2R3-S4 junos:22.3R3-S3 junos:22.4R3-S2 junos:23.2R2 junos:23.2R2-J14 junos:23.4R2 junos:24.1R2 junos:24.2R1
1795964	The rpd process crash is seen when routing-instances name length is greater than 60 characters Product-Group=junos Severity=Major	On all Junos and Junos OS Evolved platforms with Protocol Independent Multicast (PIM) enabled under Routing-instance, the Routing Protocol Daemon (rpd) process crash is seen when the routing instance (RI) name length is greater than 60 characters. Due to the rpd process crash, protocols will be impacted and traffic loss will be seen. *Resolved In:* evo:22.3R3-S3-EVO evo:23.4R2-EVO evo:24.2R1-EVO evo:24.3R1-EVO junos:22.3R3-S3 junos:23.4R2 junos:24.2R1 junos:24.3R1
PR Number	**Synopsis**	**Category: Issues related to PKI daemon**
1729592	The pkid process failed during restart. Product-Group=junos Severity=Critical	You will no longer see the PKID process restart failure during the installation of JSU package in Junos OS Evolved. *Resolved In:* evo:22.3R3-S3-EVO evo:23.2R2-EVO evo:23.4R2-EVO evo:24.1R1-EVO evo:24.2R1-EVO junos:22.1R3-S6 junos:22.3R3-S3 junos:22.4R3-S2 junos:23.2R2 junos:23.2R2-J14 junos:23.4R2 junos:24.1R1 junos:24.2R1
PR Number	**Synopsis**	**Category: Periodic Packet Management Daemon**
1480648	Junos OS and Junos OS Evolved: Flaps of BFD sessions with authentication cause a ppmd memory leak (CVE-2024-39536) Product-Group=junos Severity=Major	A Missing Release of Memory after Effective Lifetime vulnerability in the Periodic Packet Management Daemon (ppmd) of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated adjacent attacker to cause a Denial-of-Service (DoS). Please refer to https://supportportal.juniper.net/JSA82996 for more information. *Resolved In:* evo:21.2R3-S8-EVO evo:21.4R3-S7-EVO evo:22.2R3-S4-EVO evo:22.3R3-EVO evo:22.3X80-D45-EVO evo:22.3X80-D46-EVO evo:22.4R3-EVO evo:23.1R2-EVO evo:23.2R1-EVO evo:23.3R1-EVO junos:20.2R3-S9 junos:20.3X75-D36 junos:20.3X75-D52 junos:21.2R3-S8 junos:21.2X33-J2 junos:21.4R3-S7 junos:22.1R3-S4 junos:22.2R3-S4 junos:22.3R3 junos:22.4R2-S2 junos:22.4R3 junos:23.1R2 junos:23.2R1 junos:23.3R1
PR Number	**Synopsis**	**Category: PPPoE functional plugin for bbe-smgd**
1782239	After Routing Engine switchover PPPoE subscribers may fail to login Product-Group=junos	On all Junos OS on MX Platforms, after Routing Engine (RE) switchover using BNG for PPPoE (Point-to-Point Protocol over Ethernet) subscribers, may impacting customers authentication or failing to connect.

	Severity=Major	*Resolved In:* evo:23.4R2-EVO evo:24.1R1-EVO evo:24.2R1-EVO junos:19.4R3-J20 junos:19.4R3-S10-J1 junos:19.4R3-S13 junos:21.2R3-S7-J4 junos:21.2R3-S8 junos:22.1R3-S6 junos:22.3R3-S3 junos:22.4R2-S1-J6 junos:22.4R3-S1 junos:23.2R2 junos:23.4R2 junos:24.1R1 junos:24.2R1
PR Number	**Synopsis**	**Category: PTX10K Routing Engine**
1742746	[MX10008/16] 'Loss of communication with Backup RE' happens after vmhost rebooting when optical module(SFP) is used as management port. Product-Group=junos Severity=Major	The issue happens in case of using optical module (SFP) for management port. After vmhost rebooting(request vmhost reboot routing-engine both), 'Loss of communication with Backup RE' happens. Fixed versions are 24.2R1 and onward releases. *Resolved In:*
PR Number	**Synopsis**	**Category: for all ipv6 related issues**
1775394	EX/QFX: fails to ping ipv6 link local address in routing instance if there is a default route in the same instance. Product-Group=junos Severity=Major	On QFX5K, EX4300-MP, EX4400 or EX4100 series switch with VXLAN, ping to ipv6 link local address in routing instance would be failed. This issue affects only to the traffic which is sent to Link Local IPV6 Interfaces when the interface is an IRB along with VXLAN configuration. *Resolved In:* junos:22.2R3-S4 junos:22.3R3-S3 junos:22.4R3-S2 junos:23.2R2 junos:23.4R2 junos:24.1R1
PR Number	**Synopsis**	**Category: QFX L2 PFE**
1711860	The dcpfe process will crash due to memory fragmentation Product-Group=junos Severity=Major	On Junos and Junos OS Evolved platforms, the dcpfe (Dense Concentrator Packet Forwarding Engine) process crash will be observed due to memory fragmentation issue. This is a very rare case and would impact traffic as due to dcpfe failure the PFE restarts, so the interfaces will flap. *Resolved In:* evo:23.4R1-EVO junos:23.4R1
1797516	DCPFE process crash occurs in EVPN-VXLAN scenario Product-Group=junos Severity=Critical	When a vport, which is a memory pointer, is a member of an itable list, the entry in the itable should be removed before freeing the vport. For some corner case, the vport is not removed from the itable when freeing the vport. The freed memory or the reused memory corrupts the itable list and it crashes when performing some operation on the corrupted list. *Resolved In:* junos:21.4R3-S7 junos:22.1R3-S6 junos:22.2R3-S4 junos:22.3R3-S3 junos:22.4R3-S2 junos:23.2R2-S1 junos:23.4R2 junos:24.1R1 junos:24.1R2 junos:24.2R1 junos:24.3R1
PR Number	**Synopsis**	**Category: QFX L3 data-plane/forwarding**
1666260	Traffic is not restored when l2circuit configurations are deleted and added back on QFX5K Product-Group=junos Severity=Major	On the QFX5000 line of switches running Junos OS, when flapping the Layer 2 circuit (access) ports or removing and re-adding the l2 circuit configuration, the programming of the access side port fails and traffic ingressing or egressing out of it gets dropped. *Resolved In:* junos:20.2R3-S8 junos:20.4R3-S8 junos:21.2R3-S6 junos:21.3R3-S5 junos:21.4R3-S5 junos:22.1R3-S4 junos:22.2R3-S3 junos:22.3R3 junos:22.3R3-S1 junos:22.4R3 junos:23.1R2 junos:23.2R2 junos:23.3R1 junos:23.4R1
1780058	Tarffic drop observed on ipv4 and ipv6 streams ipv4 and ipv6 streams with qfx5110-32q and qfx5110-48s VC Product-Group=junos Severity=Critical	When VC is formed with qfx5110-32q and qfx5110-48s, 0.2% traffic drop issue with 40G/100G optics will be seen only with line rate traffic upon reboot *Resolved In:*
PR Number	**Synopsis**	**Category: QFX EVPN / VxLAN**
1778725	Traffic drop is observed when VIPs become	Under a rare scenario, on all Junos and Junos Evolved platforms configured with

	unreachable due to GARP sent on VLANs to which the VIP does not belong Product-Group=junos Severity=Major	EVPN-VXLAN (Ethernet Virtual Private Network-Virtual Extensible Local Area Network) type 5 routes, Bridge-Domain, IRB (Integrated Routing and Bridging) and having L4 (Layer 4 device like an application load balancer) devices as single-homed with each border leaf and when VIP (Virtual Internet Protocol) entries are learnt on a leaf and L4 failover happens, it is observed that the VIPs announced by GARP (Gratuitous Address Resolution Protocol) is sent on VLANs that the VIP does not belong to and the incorrect GARP is not handled as per the expectation. *Resolved In:* junos:21.4R3-S7 junos:22.1R3-S6 junos:22.2R3-S4 junos:22.3R3-S3 junos:22.4R3-S2 junos:23.2R2 junos:23.4R1-S1 junos:23.4R2 junos:24.1R1 junos:24.2R1
PR Number	**Synopsis**	**Category: QFX10008/16 QFX10002 Ultimat/Elit fabric related issues.**
1787486	Apstra DC Reference ERB Design: QFX10002-36Q as a BL , after restart PFE of the BLs PFE cored and after a while SIB/Fabric error observed Product-Group=junos Severity=Major	this issue is seen only if DCPFE terminates abnormally when link training is in progress. the link states are not updated in Chassisd when DCPFE cores and, when dcpfe comes up again, chassisd is trying to retrain the links already trained, hence links are being marked as fault. the chances of hitting this issue are very less because the link training period is very short. Discussions are going on to address this issue in RLI. *Resolved In:*
PR Number	**Synopsis**	**Category: QFX10008/16 QFX10002 Ultimat/Elit platform related issues -**
1797511	[JDI-RCT-EVPNVXLAN-L2Stitching]: DCPFE core observed on QFX10k while running profile baseline in 22.2R3-S3.18 image Product-Group=junos Severity=Critical	In very rare instances of a large config commit, on the QFX10002-36Q routers, the dcpfe can core due to watchdog timeout. After the core, the dcpfe respawns and the system functions normally without any manual intervention. *Resolved In:* junos:21.4R3-S9 junos:22.2R3-S4 junos:22.3R3-S3 junos:22.4R3-S3 junos:23.4R2 junos:24.2R1 junos:24.3R1
PR Number	**Synopsis**	**Category: QFX5100 Interface related issues**
1665800	Ports with SFP-T 1G plugged in may go to hung state on QFX5100 (tvp-image) platforms Product-Group=junos Severity=Major	When the remote end server/system reboots, QFX5100 platform ports with SFP-T 1G inserted may go into a hung state and remain in that state even after the reboot is complete. This may affect traffic after the remote end system comes online and resumes traffic transmission. *Resolved In:* junos:20.2R3-S7 junos:20.2R3-S8 junos:20.4R3-S6 junos:20.4R3-S7 junos:21.2R3-S3 junos:21.4R3-S3 junos:21.4R3-S4 junos:21.4R3-S6 junos:22.2R3-S1
PR Number	**Synopsis**	**Category: QFX5100 Platfom related issues. CPLD, FPGA, FRU, Host, RE**
1742565	Ports with SFP-T 1G plugged in may go to hung state on QFX5100 (non-tvp-image) platforms Product-Group=junos Severity=Major	When the remote end server/system reboots, QFX5100 platform ports with SFP-T 1G inserted may go into a hung state and remain in that state even after the reboot is complete. This may affect traffic after the remote end system comes online and resumes traffic transmission. *Resolved In:* junos:20.4R3-S10 junos:21.4R3-S5 junos:21.4R3-S6 junos:21.4R3-S9
1762937	MPLS traffic will get dropped over AE on QFX5100/EX4600 platforms Product-Group=junos Severity=Major	On QFX5100/EX4600 platforms in case of PHP, the next-hop is chosen by the PHP filter. In case of AE(Aggregate Ethernet) interfaces, PHP filter will not be updated with the correct next-hop which results into MPLS (Multi Protocol Label Switching) traffic loss. *Resolved In:* junos:20.4R3-S10 junos:21.2R3-S7 junos:21.4R3-S5 junos:21.4R3-S6
PR Number	**Synopsis**	**Category: QFX5100 Virtual Chassis**
1679919	PFE process crash might be observed on QFX5100 platforms Product-Group=junos	On QFX5100 platforms (both stand-alone and VC scenario) running Junos, occasionally during the normal operation of the device, PFE (Packet Forwarding Engine) can crash resulting in total loss of traffic. The PFE reboots itself following

	Severity=Major	the crash. *Resolved In:* junos:20.2R3-S8 junos:20.3X75-D44 junos:20.4R3-S7 junos:21.2R3-S5 junos:21.3R3-S4 junos:21.4R3-S2
PR Number	**Synopsis**	**Category: QFX5K JUNOS Interface, MACSec, Optics, SDK, PHY**
1783296	22.2R3-S3 - Traffic loss for 5 secs observed while upgrade of fpc1 in 2 member VC Product-Group=junos Severity=Major	Traffic loss for 5 secs observed while upgrade of fpc1 in 2 member VC *Resolved In:* junos:24.2R2 junos:24.3R1
PR Number	**Synopsis**	**Category: QFX5200/5110/5120/5210 Platfom issues**
1768554	Virtual chassis formation fails for VCP ports Product-Group=junos Severity=Major	On platforms that support QFX5E image and that support virtual chassis, when em0 is configured or em0 of master is plugged out, VC formation fails when network port is converted to vcp (Virtual Chassis port) port. *Resolved In:* junos:21.4R3-S5 junos:21.4R3-S6 junos:22.1R3-S5 junos:22.2R3-S3 junos:22.3R3-S2 junos:22.4R3 junos:23.2R2 junos:23.4R1 junos:23.4R2 junos:24.1R1
1783434	In qfx5110-48s-4c and qfx5120 platform when below steps are used to upgrade the system(two member Virtual-Chassis), system can have non deterministic selection of master(i.e. not based on system uptime). Product-Group=junos Severity=Major	In qfx5110-48s-4c and qfx5120 platform when below steps are used to upgrade the system(two member Virtual-Chassis), system can have non deterministic selection of master(i.e. not based on system uptime). ======= IP-Step1--Disable the uplink and downlinks from FPC-0 Switch. IP-Step2--Break the Virtual Chassis (VC) link between FPC 0 and FPC 1. IP-Step3--Initiate the upgrade process on the backup switch FPC0. IP-Step4--Swap the downlink and uplink ports by disabling them on the primary device[FPC1] and re-enabling those ports on the backup[FPC0] simultaneously. IP-Step5----Initiate the upgrade process on the Switch FPC1. IP-Step6----Bring back the Virtual chassis by enabling the VC ports. The FPC0 should become the Master at the end of STEP6 based on FPC uptime but FPC1 stays as the Master and FPC0 becomes backup. ======== *Resolved In:*
1796218	The 100G VCP will go down upon restarting or upgrading the device Product-Group=junos Severity=Major	On Junos QFX5K platforms in a Virtual Chassis scenario, the 100G VCP (Virtual Chassis Port) will go down and remain in a down state after a device or VCP restart or device upgrade. *Resolved In:* junos:22.2R3-S4 junos:24.2R2 junos:24.3R1 junos:24.4R1
PR Number	**Synopsis**	**Category: RPD Next-hop issues including indirect, CNH, and MCNH**
1562387	The session status gets stuck in the Invalid state after the core-facing link fails in the primary PE devices. Product-Group=junos Severity=Critical	Due to a race condition, the 'show multicast route extensive instance " output can display the session status as Invalid. Such an output is a cosmetic defect and not indicative of a functional issue. *Resolved In:* junos:22.4R3-S1
1777068	Policy Evaluation causing unrelated route flaps in Dynamic Tunnel setup Product-Group=junos Severity=Major	On all Junos and Junos Evolved platforms that support Dynamic tunnels, a policy evaluation of the routing policy causes flaps for unrelated tunnel routes. The route flap for the tunnel route will cause traffic loss. *Resolved In:* evo:22.2R3-S4-EVO evo:22.2X3-EVO evo:22.4R3-S1-EVO evo:23.2R2-EVO evo:23.4R2-EVO evo:24.1R1-EVO junos:20.3X75-D44 junos:20.3X75-D440 junos:22.2R3-S4 junos:22.4R3 junos:22.4R3-S1 junos:23.2R2 junos:23.2R2-J14 junos:23.4R2 junos:24.1R1
PR Number	**Synopsis**	**Category: RPD policy options**
1714163	The static routes are installed in the routing table even though interface routes are not present Product-Group=junos Severity=Critical	On all Junos and Junos OS Evolved platforms, the static routes are installed in the routing table even though the corresponding interface routes are not present. *Resolved In:* evo:23.2R2-EVO evo:23.4R1-EVO junos:22.4R3-S2 junos:23.2R2 junos:23.2R2-J14 junos:23.4R1 junos:23.4R2

PR Number	Synopsis	Category: PTX10K specific platform PRs
1735224	Junos OS Evolved: PTX10001, PTX10004, PTX10008, PTX10016: MAC address validation bypass vulnerability (CVE-2023-44190) Product-Group=junos Severity=Major	An Origin Validation vulnerability in MAC address validation of Juniper Networks Junos OS Evolved on PTX10001, PTX10004, PTX10008, and PTX10016 devices allows a network-adjacent attacker to bypass MAC address checking, allowing MAC addresses not intended to reach the adjacent LAN to be forwarded to the downstream network. Due to this issue, the router will start forwarding traffic if a valid route is present in forwarding-table, causing a loop and congestion in the downstream layer-2 domain connected to the device. Please refer to https://supportportal.juniper.net/JSA73154 for more information. *Resolved In:* evo:20.4X6-EVO evo:21.4R3-S5-EVO evo:22.1R3-S4-EVO evo:22.3R2-S2-EVO evo:22.3R3-S1-EVO evo:22.3X50-EVO evo:22.3X80-D35-EVO evo:22.3X80-D36-EVO evo:22.3X80-D37-EVO evo:22.4R2-S1-EVO evo:22.4R3-EVO evo:23.1R2-EVO evo:23.2R1-S1-EVO evo:23.2R2-EVO evo:23.3R1-EVO junos:22.4R3 junos:23.1R2 junos:23.2R2 junos:23.3R1
PR Number	**Synopsis**	**Category: Issues related to control plane security**
1780283	Junos OS and Junos OS Evolved: Loading a malicious certificate from the CLI may result in a stack-based overflow (CVE-2024-39556) Product-Group=junos Severity=Critical	A Stack-Based Buffer Overflow vulnerability in Juniper Networks Junos OS and Juniper Networks Junos OS Evolved may allow a local, low-privileged attacker with access to the CLI the ability to load a malicious certificate file, leading to a limited Denial of Service (DoS) or privileged code execution. Please refer to https://supportportal.juniper.net/JSA83016 for more information. *Resolved In:* evo:21.2R3-S8-EVO evo:22.2R3-S4-EVO evo:22.3R3-S3-EVO evo:22.3X80-D45-EVO evo:23.2R2-S2-EVO evo:23.4R1-S1-EVO evo:23.4R2-EVO evo:24.2R1-EVO junos:19.4R3-S14 junos:20.2R3-S9 junos:20.3X75-D36 junos:20.3X75-D52 junos:21.2R3-S8 junos:21.4R3-S7 junos:22.1R3-S6 junos:22.2R3-S4 junos:22.3R3-S3 junos:22.4R3-S2 junos:23.2R2 junos:23.2R2-S2 junos:23.4R1-S1 junos:23.4R1-S1-J6 junos:23.4R2 junos:24.2R1 junos:24.2R2 junos:24.3R1
PR Number	**Synopsis**	**Category: SNMP Infrastructure (snmpd, mib2d)**
1775593	Junos OS and Junos OS Evolved: Multiple vulnerabilities resolved in net-SNMP 5.9.4 (CVE-2015-5621, CVE-2008-6123) Product-Group=junos Severity=Critical	Multiple vulnerabilities have been resolved in net-SNMP software included with Juniper Networks Junos OS and Junos OS Evolved by upgrading net-SNMP to version 5.9.4, or by fixing vulnerabilities found during internal testing. Please refer to https://supportportal.juniper.net/JSA82973 for more information. *Resolved In:* evo:21.2R3-S8-EVO evo:21.4R3-S7-EVO evo:22.2R3-S4-EVO evo:22.3R3-S3-EVO evo:22.3X80-D45-EVO evo:23.2R2-EVO evo:23.4R2-EVO evo:24.1R1-EVO evo:24.2R1-EVO junos:19.1R3-S12 junos:19.2R3-S9 junos:19.3R3-S10 junos:20.2R3-S9 junos:20.3X75-D36 junos:20.3X75-D52 junos:21.2R3-S8 junos:21.4R3-S7 junos:22.1R3-S6 junos:22.2R3-S4 junos:22.3R3-S3 junos:22.4R3-S2 junos:22.4R3-S3 junos:23.2R2 junos:23.2R2-J14 junos:23.4R1-S1 junos:23.4R2 junos:24.1R1 junos:24.2R1 junos:24.2R1-S1
PR Number	**Synopsis**	**Category: Generic platform and infra issues for MS-MIC and MS-MPC(XLP)**
1714416	mspmand crashes after loading a new image Product-Group=junos Severity=Major	Once the device is loaded with the new image, PIC tries to boot up. mspmand is one of the processes inside PIC, crashes sometimes. *Resolved In:* evo:23.4R1-EVO junos:23.4R1
PR Number	**Synopsis**	**Category: Bug and Review Tracking for Segment routing traffic eng**
1763406	LDP traffic to destination route might be lost when TI-LFA is configured Product-Group=junos Severity=Major	On all Junos and Junos OS Evolved platforms, when LDP tunnel over SR-TE route or over RSVP and LFA/rLFA/TI-LFA backup path for the same destination is configured, or if rLFA/LFA with L-ISIS as backup path is configured, the route to the destination is missing. LDP route for the destination is deleted because SR-TE LSP next hop is deleted by processing L-ISIS route with the backup path. Due to this LDP route gets deleted, LDP traffic to destination route is lost. *Resolved In:* evo:21.4R3-S6-EVO evo:22.1R3-S5-EVO evo:22.3R3-S2-EVO evo:22.4R3-

		EVO evo:23.2R2-EVO evo:23.4R1-EVO evo:23.4R2-EVO evo:24.1R1-EVO junos:21.4R3-S6 junos:22.1R3-S5 junos:22.3R3-S2 junos:22.4R3 junos:23.2R2 junos:23.2R2-J14 junos:23.4R1 junos:23.4R2 junos:24.1R1
PR Number	**Synopsis**	**Category: all ipv6 dhcp bugs on srx platforms**
1770332	DHCP server not responding to some clients Product-Group=junos Severity=Critical	SRX DHCP server does not respond to some clients after upgrading to 21.4R3-S5. *Resolved In:* junos:21.2R3-S7 junos:21.4R3-S6 junos:22.1R3-S5 junos:22.4R3 junos:22.4R3-S4 junos:23.2R2 junos:23.4R1 junos:23.4R2 junos:24.1R1
PR Number	**Synopsis**	**Category: SRX branch platforms**
1713759	Continuous vmcores observed on the secondary node when committing the "set system management-instance" command Product-Group=junos Severity=Major	On Junos SRX3xx series platforms, when the "set system management-instance" command is committed on the secondary node, continuous vmcores are observed on primary and secondary nodes. No recovery action is needed for the primary node and the secondary node of the cluster reboots automatically to recover from the error. The cluster redundancy is not restored until the management-instance knob is removed using the "delete system management-instance". *Resolved In:* junos:20.4R3-S8 junos:21.2R3-S6 junos:21.2R3-S7 junos:21.3R3-S5 junos:21.4R3-S3 junos:22.1R3-S2 junos:22.2R3 junos:22.3R3 junos:22.4R2 junos:23.1R1 junos:23.1R2 junos:23.2R1
1780326	IP Monitoring fail to install route after SRX cluster reboot Product-Group=junos Severity=Major	On Junos SRX branch series platforms in cluster, the IP Monitoring fails to install route after the SRX cluster reboots. *Resolved In:* junos:21.2R3-S8 junos:21.4R3-S7 junos:22.1R3-S6 junos:22.2R3-S4 junos:22.3R3-S3 junos:22.4R3-S2 junos:23.2R2-S1 junos:23.4R1-S2 junos:23.4R2 junos:24.2R1
PR Number	**Synopsis**	**Category: SSL Proxy functionality on JUNOS**
1788673	The flowd crash will be observed when the TLS 1.3 session ticket is received on SSL-I Product-Group=junos Severity=Major	On SRX platforms with SSL (Secure Sockets Layer) Proxy configured, due to timing synchronization issues, while doing multiple session tickets check on SSL_I [initiator on the server side], and SSL_T [terminator on the client side] updating the session cache and releasing the session cache resources resulting in proxy session info cleared & causing the flowd crash at SSL_I. The issue happens when the SSL_I (Server) is using TLS1.3 and SSL_T (Client) using TLS1.2. *Resolved In:* junos:22.1R3-S6 junos:22.2R3-S4 junos:22.3R3-S3 junos:22.4R3-S2 junos:23.2R2 junos:23.4R2 junos:24.1R1 junos:24.2R1
PR Number	**Synopsis**	**Category: MPC7/8/9 Interface Issues**
1692063	PCS errors and framing errors on 100GE interfaces on certain Juniper platforms Product-Group=junos Severity=Major	On certain Junos platforms having 20.2R1 or later release, with specific PIC (Physical Interface Card)/MIC (Modular Interface Card)/FPC (Flexible PIC Concentrator), PCS (Physical Coding Sublayer) errors and framing errors would be seen on 100GE interfaces with LR4 optics or on its peer device. The framing/CRC (Cyclic Redundancy Check) errors which would be seen when the PCS error rate is high could lead to packet drops hence impacting data services. Enabling FEC (forwarding Error Correction) feature on the impacted interface may reduce the frequency of packet drop. *Resolved In:* evo:22.2R3-EVO evo:22.3R2-EVO evo:22.4R2-EVO evo:23.1R1-EVO junos:20.2R3-S2-J6 junos:20.2R3-S3-J8 junos:20.2R3-S5-J3 junos:20.2R3-S5-J4 junos:20.2R3-S7 junos:20.3X75-D46 junos:20.3X75-D46-J2 junos:20.4R3-J10 junos:20.4R3-S2-J22 junos:20.4R3-S4-J11 junos:20.4R3-S4-J6 junos:20.4R3-S5 junos:21.2R3-J13 junos:21.2R3-S2-J20 junos:21.2R3-S3 junos:21.4R1-S2-J1 junos:21.4R2-S1-J2 junos:21.4R2-S1-J5 junos:21.4R3-S2 junos:22.2R2-S1-J2 junos:22.2R3 junos:22.3R2 junos:22.4R1-S2-J1 junos:22.4R2 junos:23.1R1
PR Number	**Synopsis**	**Category: Stout card (MPC7) fabric issues**

1768592	The SFB3 will go offline during during SFB3 < -> ADC < -> MPC7E link initialization Product-Group=junos Severity=Critical	On MX2020 and MX2010 platforms with Switch Fabric Boards (SFB) 3 and Modular Port Concentrators (MPCs) MPC7E-10G or MPC7E-MRATE inserted via Adapter Card (ADC) MX2000-LC, SFB3 will go offline during SFB3 < -> ADC < -> MPC7E link initialization with a fatal error. This is a timing issue and will not be seen with every SFB3 < -> ADC < -> MPC7E link initialization. It happens because of a race condition between certain events occurring during MPC initialization. *Resolved In:* junos:21.2R3-S8-J6 junos:22.2R1-S2-J3 junos:22.2R2-S1-J2 junos:22.2R2-S1-J5 junos:22.2R3-S3-J3 junos:22.2R3-S4 junos:22.3R3-S3 junos:22.4R3-S2 junos:23.2R2-S1 junos:23.4R2 junos:24.1R2 junos:24.2R1 junos:24.3R1
1769983	At MX2020 with SFB3 and MPC7+ADC in FPC slot 11, link errors in fabric planes 1, 4, 7, 10 will be seen upon MPC7/ADC restart in FPC slot 11 Product-Group=junos Severity=Critical	On the Junos MX2020 with SFB3 and MPC7+ADC in FPC slot 11, link errors in fabric planes 1, 4, 7, and 10 will be seen upon MPC7/ADC restart in FPC slot 11. The link errors will come along with the 'failed word alignment' syslog message logged by hsl2_channel_train_hsl2_rx(). In the rare scenario, the traffic impact will be observed as some of the fabric links do not come online. *Resolved In:* junos:21.2R3-S8-J6 junos:22.2R2-S1-J2 junos:22.2R2-S1-J5 junos:22.2R3-S3-J3 junos:22.3R3-S3 junos:22.4R3-S2 junos:23.2R2-S1 junos:23.4R2 junos:24.2R1 junos:24.3R1
PR Number	**Synopsis**	**Category: MX10003/MX204 Platform SW - Chassisd s/w defects**
PR Number	**Synopsis**	**Category: SRX-1RU platfom chassisd SW defects**
1711467	SRX4600 doesn't support ae interfaces Product-Group=junos Severity=Major	On Junos SRX4600 platforms, ae interfaces doesn't come up or not work properly when configured in HA (High Availability) cluster mode. *Resolved In:* junos:20.2R3-S9 junos:20.4R3-S10 junos:21.2R3-S5 junos:21.3R3-S4 junos:21.4R3-S3 junos:22.1R3-S2 junos:22.2R3 junos:22.3R3 junos:22.4R2 junos:23.1R1 junos:23.2R1
PR Number	**Synopsis**	**Category: SRX-1RU infrastructure SW defects**
1784983	Chassis alarm not present for if /var partition usage exceeds 100% Product-Group=junos Severity=Major	When /var partition disk space is greater than 100%, "RE 0 /var partition usage is high" chassis alarm gets cleared *Resolved In:* junos:21.2R3-S8 junos:21.4R3-S7 junos:22.1R3-S6 junos:22.2R3-S4 junos:22.3R3-S3 junos:22.4R3-S2 junos:23.2R2 junos:23.4R1-S1 junos:23.4R2 junos:24.1R1 junos:24.2R1
PR Number	**Synopsis**	**Category: SRX-1RU platfom datapath SW defects**
1732876	Traffic drops will be observed when a BGP session comes up after the network flap Product-Group=junos Severity=Critical	On SRX platforms with BGP (Border Gateway Protocol) multipath and forwarding table policies configured, for the type 5 EVPN-VXLAN (Ethernet VPN-Virtual Extensible LAN) tunnel routes traffic drops will be observed for a few composite next-hop that are not installed in PFE (Packet Forwarding Engine) when a BGP session comes up after the network flap. The issue can also happen when deactivating/activating OSPF (Open Shortest Path First) in the OSPF environment. *Resolved In:* junos:23.2R2 junos:23.2R2-S1 junos:23.4R1 junos:23.4R2 junos:24.1R1
PR Number	**Synopsis**	**Category: Issues related to broadband edge apps (PPP, DHCP) on ZT/YT**
1774026	MX304 - messages seen - No tunnel entry found for received L2TP tunnel control packet Product-Group=junos Severity=Minor	BBE on MX304 Platform is supported from 23.2 Release onwards *Resolved In:*
PR Number	**Synopsis**	**Category: ZT/YTpfe bridging, learning, stp, oam, irb software**

1761792	High heap memory utilization is observed on FPC's, when high-scaled logical interfaces and scaled vlan inner-list per logical interface is configured Product-Group=junos Severity=Major	On all MX platforms with line cards MPC10/MPC11/LC9600/MX304, high heap memory utilization on FPC with high-scaled double-tagged IFL (logical interface) configuration. The issue occurs because the configuration of scaled inner vlan-list (a large range) along with corresponding high-scaled logical interfaces creates as high as 14 million or more double-tagged streams. This results in high memory utilization on the FPC. *Resolved In:* evo:23.4R2-EVO evo:24.1R1-EVO junos:22.4R3 junos:23.2R2 junos:23.4R1-S1 junos:23.4R2 junos:24.1R1
1792736	Transit traffic does not get forwarded in EVPN-VxLAN scenario on Junos MX/EX platforms Product-Group=junos Severity=Major	On Junos MX240/MX480/MX960/MX2008/MX10004/MX10008/MX2010/MX2020 platforms with MPC10E/11E/LC9600 line cards and MX304 platform and EX9204/EX9208/EX92014 with EX9200-15C line card, in Ethernet Virtual Private Network-Virtual Extensible LAN (EVPN-VxLAN) scenario the transit traffic does not get forwarded due to incorrect inner ethernet header. *Resolved In:* evo:23.4R2-EVO evo:24.2R1-EVO evo:24.3R1-EVO junos:22.4R3-S3 junos:23.2R2-S1 junos:23.4R2 junos:24.2R1 junos:24.3R1
PR Number	**Synopsis**	**Category: ZT/YT pfe l3 forwarding issues**
1670797	Junos OS: MX Series: Gathering statistics in a scaled SCU/DCU configuration will lead to a device crash (CVE-2024-21603) Product-Group=junos Severity=Major	An Improper Check for Unusual or Exceptional Conditions vulnerability in the kernel of Juniper Network Junos OS on MX Series allows a network based attacker with low privileges to cause a denial of service. Please refer to https://supportportal.juniper.net/JSA75744 for more information. *Resolved In:* evo:22.1R3-EVO evo:22.2R2-EVO evo:22.3R2-EVO evo:22.4R1-EVO junos:19.1R3-S11 junos:19.2R3-S8 junos:19.3R3-S8 junos:19.4R3-S13 junos:20.3X75-D44 junos:20.3X75-D46 junos:20.4R3-S9 junos:21.2R3-S6 junos:21.3R3-S5 junos:21.4R3 junos:22.1R3 junos:22.2R2 junos:22.3R2 junos:22.4R1
PR Number	**Synopsis**	**Category: Issues related to broadband edge apps (PPP, DHCP) on Trio ch**
1715420	In L2TP, link control protocol connection problems were observed with IPv4 and IPv6 control protocol termination requests and IPv6 control protocol connections. Product-Group=junos Severity=Major	On all MX platforms with MPC10/MPC11/LC9600 line cards and MX304, L2TP (Layer 2 Tunnel Protocol) LNS (L2TP network server) link control protocol connection issues like the connection being dropped due to incorrect VBF type (Variable Based Flow) observed with IPv4 and IPv6 CP (CP - Control Protocol) termination requests and IPv6CP connections. *Resolved In:* evo:23.1R2-EVO evo:23.2R1-EVO evo:23.3R1-EVO junos:22.4R3 junos:23.1R2 junos:23.2R1 junos:23.3R1
1722945	PADT response will not be sent for an incoming PPPoE/PPP data Packet from an unknown session ID Product-Group=junos Severity=Major	On all MX platforms with line cards before MPC10, when Broadband Network Gateway (BNG) switchover occurs, the new master does not send PPPoE Active Discovery Termination (PADT) packet for an unknown session if the incoming packet is PPPoE/PPP data packet and thus the existing subscribers does not come up on this router. *Resolved In:* junos:21.3R3-S5 junos:21.4R3-S6 junos:22.4R3 junos:23.1R2 junos:23.2R2 junos:23.3R1 junos:23.4R1
PR Number	**Synopsis**	**Category: Trio pfe bridging, learning, stp, oam, irb software**
1745803	During multicast traffic flow , 'sw error' discard count is incrementing continuously Product-Group=junos Severity=Major	On all MX series platforms, Multicast over IRB with receivers spanning across PFEs then some vty exception counters which keeps incrementing. *Resolved In:* junos:21.2R3-S8 junos:21.4R3-S7 junos:22.1R3-S6 junos:22.3R3-S3 junos:22.4R3-S1 junos:22.4R3-S2 junos:23.2R2 junos:23.4R2 junos:24.1R1
PR Number	**Synopsis**	**Category: DDos Support on MX**
1733477	Harmless logs "DDOS : Failed to insert flow to lkup map for proto: 3c00" observed in syslog Product-Group=junos Severity=Major	"Failed to insert flow to lkup map for proto: 3c00" messages reported repeatedly in the syslog/messages file without any functional impact. *Resolved In:* evo:21.4R3-S6-EVO evo:23.4R2-EVO evo:24.1R1-EVO junos:21.4R3-S7

junos:22.4R3-S2 junos:23.2R2 junos:23.4R2 junos:24.1R1

PR Number	Synopsis	Category: UI Infrastructure - mgd, DAX API, DDL/ODL
1736976	qfx goes into amnesiac after a power outage and commit errors for scripts prevent recovery Product-Group=junos Severity=Major	On all Junos platforms, the group file /etc/backup/group and the directory /var/etc/ are becoming corrupt, causing the mgd initialization to fail during system boot. This rare issue occur due to an abrupt power outage occurring while the files were being written. *Resolved In:* junos:21.4R3-S7 junos:22.2R3-S4 junos:23.2R2 junos:23.4R2 junos:24.1R1
1770643	RPD core seen when groups is activated before corresponding 'apply-groups' in configuration Product-Group=junos Severity=Major	On all Junos and Junos Evolved platforms, when the group is activated after the corresponding 'apply-groups' statement configuration, rpd core is seen. *Resolved In:* evo:21.2R3-S8-EVO evo:21.4R3-S8-EVO evo:22.2R3-S3-EVO evo:22.2X100-D20-EVO evo:22.3R3-S3-EVO evo:22.3X50-EVO evo:22.3X80-D43-EVO evo:22.3X80-D44-EVO evo:22.4R3-S1-EVO evo:23.2R2-EVO evo:23.4R2-EVO evo:24.1R1-EVO junos:21.2R3-S8 junos:21.2X32-D30 junos:21.4R3-S8 junos:22.2R3-S4 junos:22.3R3-S3 junos:22.4R3-S1 junos:22.4R3-S2 junos:23.2R2 junos:23.4R1-S1 junos:23.4R2 junos:24.1R1
PR Number	**Synopsis**	**Category: Issues related to NETCONF**
1585855	< ok/> response is getting generated along with < rpc-error> Product-Group=junos Severity=Critical	When maximum-password-length is configured and the user tries to configure password whose length exceeds configured maximum-password-length, there is an error and the " tag is emitted. (Ideally " tag should not be emitted in an error scenario.) The configuration does not get committed. *Resolved In:* evo:22.2R3-S1-EVO evo:22.3R2-S2-EVO evo:22.3X50-EVO evo:22.3X80-D43-EVO evo:22.3X80-D44-EVO evo:22.4R3-EVO evo:23.1R1-EVO evo:23.2R1-EVO junos:20.3X75-D36 junos:22.1R3-S6 junos:22.2R3-S1 junos:22.3R2-S2 junos:22.3R3-S1 junos:22.4R2-S2 junos:22.4R3 junos:23.1R1 junos:23.2R1 junos:23.4R2
PR Number	**Synopsis**	**Category: Junos Fusion Aggregation Device Infra**
1787147	The sdp process crashes when trying to add a new satellite device to the network Product-Group=junos Severity=Major	In the Junos Fusion setup, the sdp (Satellite Discovery and Provisioning Daemon) process crashes repeatedly when trying to add a new satellite device to the network. This issue happens when the MD5 encrypted data is read as a string, in which the string validation code throws errors when the first byte of MD5 encrypted data is 0. *Resolved In:* evo:24.1R1-EVO evo:24.2R1-EVO junos:21.2R3-S8 junos:21.4R3-S7 junos:22.1R3-S6 junos:22.2R3-S4 junos:22.3R3-S3 junos:22.4R3-S2 junos:23.2R2 junos:23.4R2 junos:24.1R1 junos:24.2R1
PR Number	**Synopsis**	**Category: MX10K linecard**
1785182	On Junos MX and SRX platforms silent FPC reboot is observed with no generation of crash files Product-Group=junos Severity=Major	On Junos platforms with MPC7E, MPC8E, MPC9E. LC1201, LC480, MS-SPC3, SRX5K-SPC3 cards. When one of these line cards have uncorrectable memory issue, the line card reboots silently without generating any crash files. *Resolved In:* junos:21.2R3-S9 junos:22.4R3-S2 junos:23.2R2-S1 junos:23.4R2 junos:23.4R2-S1 junos:24.1R2 junos:24.2R1 junos:24.3R1
PR Number	**Synopsis**	**Category: PTX/QFX100002/8/16 platform software**
1642645	[resiliency] [cm_infra] PTX10008 :: Verifying error counters failed as they are not in expected count due to an additional row for "OC-category" in "show chassis errors active detail" Product-Group=junos Severity=Major	. *Resolved In:* evo:22.1R1-EVO evo:22.1R2-EVO evo:22.2R1-EVO evo:22.3R1-EVO junos:22.1R1 junos:22.1R2 junos:22.2R1 junos:22.3R1

PR Number	Synopsis	Category: For GPRS security features on highend SRX series
1736985	Cores are observed on both the nodes of SRX HA cluster setup when it's upgraded to 21.2 and above Product-Group=junos Severity=Critical	On Junos SRX high-end platforms configured with GTP (GPRS Tunneling Protocol), during the upgrade of an SRX High Availability (HA) cluster, a crash occurs on the nodes when processing GTP packet traffic. This persistent crashing prevents the system from restarting and impacts service availability. *Resolved In:* junos:21.2R3-S7 junos:21.4R3-S7 junos:22.1R3-S6 junos:22.3R3-S3 junos:22.4R3-S2 junos:23.2R2 junos:23.4R2 junos:24.1R1 junos:24.2R1
PR Number	**Synopsis**	**Category: VMHOST platforms software**
1726775	Upgrading the i40e NVM Firmware on Routing Engines with VM Host Support Product-Group=junosvae Severity=Minor	This change allow you to upgrade the i40e NVM firmware directly from version 4.26 to version 7.00. (for example, when upgrade from Junos 18.2 to Junos 21.3) You don't need to upgrade the i40e NVM Firmwares with intermediated steps as described in the VMhost NVM Upgrade *Resolved In:* junos:21.4R3-S4 junos:21.4R3-S5 junos:21.4R3-S7 junos:22.1R3-S3 junos:22.2R3-S1 junos:22.3R2-S1 junos:22.3R3 junos:22.4R3 junos:23.1R2 junos:23.2R2 junos:23.3R1 junos:23.4R1
PR Number	**Synopsis**	**Category: VSRX platform software**
1079742	VRRP is not supported on vSRX which is based on VMware hypervisors Product-Group=junos Severity=Critical	VRRP is not supported on vSRX instances based on VMware hypervisors because VMware does not support virtual MAC addresses. *Resolved In:*
PR Number	**Synopsis**	**Category: Express ZX PFE L3 Features**
1732283	Junos OS Evolved: PTX10003 Series: MAC address validation bypass vulnerability (CVE-2023-44189) Product-Group=junos Severity=Critical	An Origin Validation vulnerability in MAC address validation of Juniper Networks Junos OS Evolved on PTX10003 Series allows a network-adjacent attacker to bypass MAC address checking, allowing MAC addresses not intended to reach the adjacent LAN to be forwarded to the downstream network. Due to this issue, the router will start forwarding traffic if a valid route is present in forwarding-table, causing a loop and congestion in the downstream layer-2 domain connected to the device.Please refer to https://supportportal.juniper.net/JSA73153 for more information. *Resolved In:* evo:21.4R3-S4-EVO evo:21.4X1-EVO evo:22.1R3-S3-EVO evo:22.3R2-S2-EVO evo:22.3R3-S1-EVO evo:22.3X50-EVO evo:22.3X80-D35-EVO evo:22.4R2-S1-EVO evo:22.4R3-EVO evo:23.1R2-EVO evo:23.2R1-EVO evo:23.2R2-EVO evo:23.3R1-EVO junos:22.3R2-S2 junos:22.3R3-S1 junos:22.4R2-S1 junos:22.4R3 junos:23.1R2 junos:23.2R1 junos:23.2R1-S1 junos:23.2R2 junos:23.3R1

22.2R3-S3 - List of Fixed issues Confidential

PR Number	Synopsis
1655192 SIRT=no	JUNOS build on FreeBSD 13 systems. resolution: fixed resolution reason: Fix submitted Product-Group=junos
PR Number	**Synopsis**
1688251 SIRT=no	BTB: [Supportability] Enhanced RSI for EX BCM - Feature LACP resolution: fixed

	resolution reason: Fix submitted Product-Group=junos
1775629 SIRT=yes	UNINIT:DEV_COMMON_BRANCH resolution: fixed resolution reason: Fix submitted Product-Group=junos

PR Number	Synopsis
1666687 SIRT=no	[evpn-vxlan][oism] Verifying the traffic on IXIA is failing due to traffic loss at RX port (of stc port1) resolution: fixed resolution reason: Fix submitted Product-Group=junosvae
1760898 SIRT=no	JDI-RCT:- Observed syslog error "vlan-id(38) to bd-id mapping doesn't exist in itable" after loading EVPN-VXLAN config with End_To_End profile. resolution: fixed resolution reason: Fix submitted Product-Group=junos

PR Number	Synopsis
1734263 SIRT=no	Ex-Hardening: Loopback interface configured with speed doesnt come up resolution: fixed resolution reason: Fix submitted Product-Group=junos
1759360 SIRT=no	EX hardening: EX4300-48MP Link/Activity LED is not lit when it transits to the factory default configuration by pressing the Factory Reset/Mode bu resolution: fixed resolution reason: Fix submitted Product-Group=junosvae
1781409 SIRT=no	[interface] [all] EX4300-48MP :: JUNOS_REG: [EX4300-48MP]:Interfaces are not coming up after channelization on ex4300-48mp Device resolution: fixed resolution reason: Fix submitted Product-Group=junos

PR Number	Synopsis
1715664 SIRT=no	[EX9204] supported SNMP OIDs for jnxPsuObjects on ex92xy platforms resolution: fixed resolution reason: Fix submitted Product-Group=junos

PR Number	Synopsis
1705504 SIRT=no	remote-port-mirroring option to be removed from set forwarding-options port-mirroring resolution: fixed resolution reason: Fix submitted Product-Group=junos
1719519 SIRT=no	EX3400 - vrrp backup keep changing mastership when authentication is enabled resolution: fixed resolution reason: Fix submitted Product-Group=junos
1738853 SIRT=no	Fix compilation warning due to double definition of two parameters in tvp_ngaccess_dst_pfe_bcm.c resolution: fixed resolution reason: Fix submitted Product-Group=junos
1744485 SIRT=no	EX3400 VC: "fpc1 (pkt tx) vcp get failed(100) modid 3 anchor-fpc 2 sts 100" syslog error message flooded on the system on loading MFT config resolution: fixed resolution reason: Fix submitted Product-Group=junos

1755787 SIRT=no	output option under set forwarding-options port-mirroring instance is not supported & needs to be hidden resolution: fixed resolution reason: Fix submitted Product-Group=junos
1762694 SIRT=no	[EX2300 - 22.4R1-S2.1]- When PVLAN is enabled ARP is getting re-injected along with mac-moves resolution: fixed resolution reason: Fix submitted Product-Group=junos
1765152 SIRT=no	CCL:EX2300: Traffic is completely dropped in PFE after restarting l2cpd-service resolution: fixed resolution reason: Fix submitted Product-Group=junos
1767735 SIRT=no	EX2300: dhcp clients moved to bound state, even when the source mac-address is not listed in accept-source-mac list. resolution: fixed resolution reason: Fix submitted Product-Group=junos
1771692 SIRT=yes	Dot1x Port Allows Traffic before Authentication Starts resolution: fixed resolution reason: Fix submitted Product-Group=junos
1775097 SIRT=no	JUNOS_REG: EX2300-48MP: ospf3 neighbor state are stuck in exstart state for some irb instances after configuring rip, irb resolution: fixed resolution reason: Fix submitted Product-Group=junos
1782297 SIRT=no	[EX3400][Q-in-Q][macsec] L2PT over macsec over QinQ resolution: fixed resolution reason: Fix submitted Product-Group=junos

PR Number	Synopsis
1708952 SIRT=no	EX3400: CPLD version is not showing resolution: fixed resolution reason: Fix submitted Product-Group=junos
1723768 SIRT=no	Interface: Remote side of link remains UP even after the local DUT is rebooted resolution: fixed resolution reason: Fix submitted Product-Group=junos
1741021 SIRT=no	snmp mib walk for fan related OIDs are showing incorrect values in EX2300. resolution: fixed resolution reason: Fix submitted Product-Group=junos
1742213 SIRT=no	[EI_Y] [HW] [] EX3400 jfirmware upgrade for CPLD resolution: fixed resolution reason: Fix submitted Product-Group=junos
1752625 SIRT=no	JUNOS_REG:EX2300-48MP:: Auto Negotiation state of the interface is showing as "incomplete" after applying the speed 1g when link mode full-du and half-duplex are configured resolution: fixed resolution reason: Fix submitted Product-Group=junos
1774521 SIRT=no	To have "show system memory" as part of RSI resolution: fixed resolution reason: Fix submitted Product-Group=junos

PR Number	Synopsis
1758328 SIRT=no	EX4650 VC: Members present in network mode in virtual-chassis which is not supported resolution: fixed resolution reason: Fix submitted Product-Group=junosvae
1777019 SIRT=no	Misleading logging of mode syslog on executing "show virtual-chassis mode" resolution: fixed resolution reason: Fix submitted Product-Group=junos

PR Number	Synopsis
1772982 SIRT=no	JDI:RCT:IPCLOS:TanzaniteVC/Napanook_merus_VC:contrinous tarffic drop observed on ipv4 and ipv6 streams resolution: fixed resolution reason: Fix submitted Product-Group=junos

PR Number	Synopsis
1716403 SIRT=no	Tracking RLI 54150: L2 debug enhancements: Create a separate circular kernel buffer for L2 module debug use(dev-only) resolution: fixed resolution reason: Fix submitted Product-Group=junos
1721746 SIRT=	Tracking RLI 39938: cSRX: Support ARM processor resolution: fixed resolution reason: Fix submitted Product-Group=junos
1741574 SIRT=	Tracking RLI-55117: SSL Proxy: multiple enhancement in SSL proxy/SSL stack resolution: fixed resolution reason: Fix submitted Product-Group=junos

PR Number	Synopsis
1755615 SIRT=yes	SECINTEL_NETWORK_CONNECT_FAILED Causing DAG addresses to drop to 0 entries on IPv4 resolution: fixed resolution reason: Fix submitted Product-Group=junos

PR Number	Synopsis
1720900 SIRT=no	srx5400[spc3] Multicast route group does not display Forwarding statistics counters value. resolution: fixed resolution reason: Fix submitted Product-Group=junos
1774495 SIRT=no	SPC3 stuck to boot after failing to sync Timezone with RE resolution: fixed resolution reason: Fix submitted Product-Group=junos
1774952 SIRT=no	SPC3 minor errors ASIC Error detected errorno 0x00310012 resolution: fixed resolution reason: Fix submitted Product-Group=junos
1780542 SIRT=no	Seeing one of the SPC3 card get stuck while rebooting node1 resolution: fixed

	resolution reason: Fix submitted Product-Group=junos
PR Number	**Synopsis**
1732028 SIRT=yes	Flowd coredumps after upgrading to 22.1R3 resolution: fixed resolution reason: Fix submitted Product-Group=junos
PR Number	**Synopsis**
1730751 SIRT=no	23.3DCB:SPECTRE:HA:Node1 not going to disabled state, when Disable/enable HA control-link from CLI on SRX1600, SRX1500 resolution: fixed resolution reason: Fix submitted Product-Group=junos
1740833 SIRT=no	Spectre: Putting the control link back within the heartbeat threshold/Interval time after pulling it out, The RGs are still going in ineligible and eventually in disabled state. resolution: fixed resolution reason: Fix submitted Product-Group=junos
PR Number	**Synopsis**
1710933 SIRT=no	incorrect ALB statistics - Adjusts and Updates counters misbehavior on MPC10E resolution: fixed resolution reason: Fix submitted Product-Group=junos
1718859 SIRT=no	DT_BNG: Accounting-options routing-engine-profile reprofile 'start-time' is not working as expected resolution: fixed resolution reason: Fix submitted Product-Group=junos
PR Number	**Synopsis**
1673324 SIRT=no	KERN_ARP_ADDR_CHANGE log gone resolution: fixed resolution reason: Fix submitted Product-Group=junos
PR Number	**Synopsis**
1750230 SIRT=no	JDI-RCT:MPC10E:Timeout "error: timeout communicating with Aftd-trio daemon daemon" when issuing "show l2 manager vnid lsysid 1" in mpc10 vt mode. resolution: fixed resolution reason: Fix submitted Product-Group=junos
PR Number	**Synopsis**
1681871 SIRT=no	gNMI dialout | Streaming data is received after deactivating the 2nd server resolution: fixed resolution reason: Fix submitted Product-Group=junos

1713512 SIRT=no	[Google]: JSD not accepting the client connections, even if it accepts bounces the connection resolution: fixed resolution reason: Fix submitted Product-Group=junos
1727576 SIRT=no	CMIS: PTX5k/PTX1k : 22.3R2-S1: JDI-PDT: gaft > show network-agent statistics gnmi detail display incorrect latency value resolution: fixed resolution reason: Fix submitted Product-Group=junos
1739915 SIRT=no	RLI-54431 : [Dot1x] : Dot1x Native Streaming path of few leaf parameters gets changed when egress vlan is configured resolution: fixed resolution reason: Fix submitted Product-Group=junos
1747029 SIRT=no	gRPC/TLS: JUNOS Client sets RST flag triggering connection teardown resolution: fixed resolution reason: Fix submitted Product-Group=junos
1761554 SIRT=no	[qfx5120-48y] IFA 2.0 telemetry profile not found brcm_dfw_ifa_filter_list not created resolution: fixed resolution reason: Fix submitted Product-Group=junos
1763088 SIRT=no	PDT: OBS: xmlproxyd crash seen on streaming sensors with GNMIC and JTIMON resolution: fixed resolution reason: Fix submitted Product-Group=junos

PR Number	Synopsis
1689830 SIRT=no	[timing] [hybrid] MX10004 :: MX10004 - Alfa Romeo - Huge phase jump seen when moving from primary to secondary link on AE slave link resolution: fixed resolution reason: Fix submitted Product-Group=junos

PR Number	Synopsis
1766899 SIRT=no	Synopsis: JDI-RCT:M/MX: Observed core-NGMPC0.gz.core.0 @ 0x1117fe70 in mtip_cgpcs_lnk_get_handle (ifd=0x25ff2cc8) at ../../../../../../../../src/pfe/common/drivers/mtip/mtip_cgpcs_lnk.c:41 resolution: fixed resolution reason: Fix submitted Product-Group=junos

PR Number	Synopsis
1759952 SIRT=no	DT_BNG - ancpd crash after clearing neighbor + show command - ancpd_ui_emit_subscriber_brief / ancpd_smgd_emit_proto_subscriber_mapping ancpd_smgd_timer_expiry resolution: fixed resolution reason: Fix submitted Product-Group=junos

PR Number	Synopsis
1752919 SIRT=no	MIST:APPQOE:Passive-ongoing-sessions reference count is not resetting forever when device up and running with active-probe only solution and nc passive probe sessions are in device. resolution: fixed resolution reason: Fix submitted Product-Group=junos
1756362 SIRT=no	Flowd Core observed at appqoe_app_find_best_path during L7 horizontal Testing resolution: fixed resolution reason: Fix submitted

	Product-Group=junos
1756712 SIRT=no	22.2R3-S2 :SDWAN: Core-lcore observed on testing active probe with scaled sessions resolution: fixed resolution reason: Fix submitted Product-Group=junos
1768567 SIRT=no	23.2R2:APPQOE:Passive Probe Sessions is not incrementing which is unexpected behavior. resolution: fixed resolution reason: Fix submitted Product-Group=junos
PR Number	**Synopsis**
1691237 SIRT=no	EVPN-PCT: l2ald cored at l2ald_mlrn_ifl_create, l2ald_mac_lrn_iflm_handler resolution: fixed resolution reason: Fix submitted Product-Group=junos
1692850 SIRT=no	JDI-RCT:M/Mx: fpc core @ l2alm_get_bd_current_mac_seq_number , l2alm_bd_add resolution: fixed resolution reason: Fix submitted Product-Group=junos
PR Number	**Synopsis**
1769374 SIRT=no	SRX4600 || GOLDMAN SACHS - JERSEY CITY || 22.3R1-S2.3 || SRX4600 access cluster MIB2D_COUNTER_DECREASING warning resolution: fixed resolution reason: Fix submitted Product-Group=junos
PR Number	**Synopsis**
1742344 SIRT=no	SRX5K: minor alarm not seen when rescue config is not set or deleted resolution: fixed resolution reason: Fix submitted Product-Group=junos
PR Number	**Synopsis**
1788317 SIRT=no	SRX5600 SCB slot 0 consuming more power than expected. resolution: fixed resolution reason: Fix submitted Product-Group=junos
PR Number	**Synopsis**
1680790 SIRT=no	EM Policy enhancement for Fire Temp Condition resolution: fixed resolution reason: Fix submitted Product-Group=junos
PR Number	**Synopsis**
1759393 SIRT=no	DT_BNG: stuck VIF in case no PPPoE-IA is sent on ALI VLAN resolution: fixed resolution reason: Fix submitted Product-Group=junos
PR Number	**Synopsis**

1741815 SIRT=no	Timestamp in bbe-smgd trace logs needs to include milliseconds resolution: fixed resolution reason: Fix submitted Product-Group=junos

PR Number	Synopsis
1734422 SIRT=no	Repd core @repd_mirror_compression_thread_loop on VCM member resolution: fixed resolution reason: Fix submitted Product-Group=junos
1743735 SIRT=no	JDI-RCT:RPD core "mmf_node_validate (mmf=, offset=, offset@entry=65536) at ../../../../../../src/junos/lib/libmmf/mmf.c:1124 seem when upgrading the image in mx10003 box. resolution: fixed resolution reason: Fix submitted Product-Group=junos
1762685 SIRT=no	[technology/DT/dt_Template.xml] [core] MX960 :: repd cores cause ISSU to Abort when going from 21.2 to 23.2 resolution: fixed resolution reason: Fix submitted Product-Group=junos

PR Number	Synopsis
1751665 SIRT=no	rnh_request: unexpected old opaque type: 3 message on every subscriber login resolution: fixed resolution reason: Fix submitted Product-Group=junos

PR Number	Synopsis
1753856 SIRT=no	RSMON Patricia tree ifd entries point to same shared memory index resolution: fixed resolution reason: Fix submitted Product-Group=junos
1771815 SIRT=no	Incorrect output of heap consumption in cli "show system resource-monitor summary " resolution: fixed resolution reason: Fix submitted Product-Group=junos

PR Number	Synopsis
1773913 SIRT=no	snmp mib walk for jnxSubscriberSlotTotalCounter (1.3.6.1.4.1.2636.3.64.1.1.1.9.1.2) is not working properly resolution: fixed resolution reason: Fix submitted Product-Group=junos

PR Number	Synopsis
1633505 SIRT=no	> show bfd session address | display xml rpc showing "session_addr" it should be "session-addr". resolution: fixed resolution reason: Fix submitted Product-Group=junos
1771784 SIRT=no	JUNOS_REG: MX480: Observed rpd core@ __raise, __mem_assert, task_block_free_jemalloc, task_block_free, bfd_process, task_job_run_commor task_job_run_job_bg resolution: fixed resolution reason: Fix submitted Product-Group=junos

PR	Synopsis

Number	
1652697 SIRT=no	mpls.0 route churn happens every time a labeled BGP route is re-evaluated for export even when there is no route change resolution: fixed resolution reason: Fix submitted Product-Group=junos
1691906 SIRT=no	RPD core@bgp_obread_resp_process -> io_read -> io_queue_is_stopped -> io_session_queue () resolution: fixed resolution reason: Fix submitted Product-Group=junos
1703445 SIRT=yes	BGP flaps with cisco peer with "invalid attribut list" when family traffic-engineering is added resolution: fixed resolution reason: Fix submitted Product-Group=junos
1708088 SIRT=yes	BGP Error Handling when Aggregator attribute has ASN zero (0) as a value resolution: fixed resolution reason: Fix submitted Product-Group=junos
1722367 SIRT=no	RPD core@bgp_rt_policy_afmetrics -> bgp_rt_policy_afmetrics -> bgp_labeled_common_setup_af_outmetrics -> bgp_find_out_label -> bgp_extract_gateway -> rt_nexthops_extract_gateway -> task_assert () resolution: fixed resolution reason: Fix submitted Product-Group=junos
1739010 SIRT=yes	RPD soft assert caused by delete_pending handling @bgp_rt_change -> bgp_ribgroup_change_rt -> rt_change_parms -> rt_event_change -> rt_notbest_sanity -> task_assert_soft () resolution: fixed resolution reason: Fix submitted Product-Group=junos
1742203 SIRT=no	BGP-CT with DTM: color values >16bit should not be configurable resolution: fixed resolution reason: Fix submitted Product-Group=junos
1749280 SIRT=no	As of JunOS 21 (both normal and -evo variants), a new top level operational "show routing" command was added to view the transport-class information, caused the customer behavior concern resolution: fixed resolution reason: Fix submitted Product-Group=junos
1750030 SIRT=no	[EVO_NSR_SCALE]BGP Sessions flap detected on new master RE for NSR switchover with route advertisement(Broken pipe(32) error) resolution: fixed resolution reason: Fix submitted Product-Group=junos
1752594 SIRT=yes	Deletion of routing-instance with 5K paths per prefix takes a long time with RPD cpu usage at 100% resolution: fixed resolution reason: Fix submitted Product-Group=junos
1753233 SIRT=no	Route Dampening for IBGP family inet-vpn not working when peering with RR resolution: fixed resolution reason: Fix submitted Product-Group=junos
1754178 SIRT=no	Need to set rt_data as null before deleting cloned mpls.0 rouet resolution: fixed resolution reason: Fix submitted Product-Group=junos
1758533 SIRT=no	Routes of a closing peer could lead to very slow BGP route advertisement resolution: fixed resolution reason: Fix submitted Product-Group=junos

1758542 SIRT=no	BGP delay-route-advertisement might not work mrto routes selected for UPDAE prefix packing resolution: fixed resolution reason: Fix submitted Product-Group=junos
1762515 SIRT=no	[DEV PR] BGP Multipath is not calculated when we receive immediate cb from resolver in teardown path resolution: fixed resolution reason: Fix submitted Product-Group=junos
1767612 SIRT=no	JDI-RCT:M/Mx: rpd core @bgp_shard_rcv_standby_label_resp_from_main -> bgp_shard_process_unsolicited_standby_label_resp -> bgp_shard_dequeue_shard_standby_label_awaiting_release -> hbt_delete () resolution: fixed resolution reason: Fix submitted Product-Group=junos
1769723 SIRT=no	RPD core@rt_flash_update_callback -> bgp_lbl_flash_cb -> bgp_lbl_flash_rth -> bgp_lbl_flash_rth_outlabel_node -> bgp_label_node_adjust_ppl_transit_rt () resolution: fixed resolution reason: Fix submitted Product-Group=junos
1772914 SIRT=no	[JSANITIZER]: ASAN Error observed for layer3/usr.sbin/rpd/lib/policy/com_config.c @ Line:1244 resolution: fixed resolution reason: Fix submitted Product-Group=junos
1781184 SIRT=no	BGP route updates are stuck in OutQ when the router upgraded to 20.3X75-D44.7 from 20.3X75-D43.15 resolution: fixed resolution reason: Fix submitted Product-Group=junos

PR Number	Synopsis
1737014 SIRT=no	[APPLE] - After frequent deactivate/activate bmp, few bmp sessions are struck in cleanup state resolution: fixed resolution reason: Fix submitted Product-Group=junos

PR Number	Synopsis
1739174 SIRT=no	Customer is unable to upgrade 5 units of QFX5120-48T-6C resolution: fixed resolution reason: Fix submitted Product-Group=junosvae

PR Number	Synopsis
1709606 SIRT=no	Include server name extension in the TLS Client Hello if tls-peer-name configuration is present resolution: fixed resolution reason: Fix submitted Product-Group=junos
1724732 SIRT=no	[technology/DT] [show] MX960 :: PPPoE subscribers go down post GRES in 5.5k ESSMD , 10K PPPOE steady subscribers testing resolution: fixed resolution reason: Fix submitted Product-Group=junos
1748600 SIRT=no	BNG CUPS: PVT_CP_SCALE_OUT: K8 CP authd core (AddressPoolManager:: AddressPoolManagerServicer:: Stub:: ModifyDomain ... apm.grpc.pb.cc: after changing "address-pool-manager inet" address. Authd was indicating APM "domain not ready" during DHCP logins. resolution: fixed resolution reason: Fix submitted

	Product-Group=junos
1758768 SIRT=no	Authd core when using APM for Pools in 22.4R3 resolution: fixed resolution reason: Fix submitted Product-Group=junos

PR Number	Synopsis
1731617 SIRT=no	EVPN-VxLAN: CRB: Observing traffic drops on the system in convergence test after bringing the flapped link back up again resolution: fixed resolution reason: Fix submitted Product-Group=junos

PR Number	Synopsis
1778400 SIRT=no	Qfx5220-32CD: telemetry sensor /junos/system/linecard/qmon-sw not working resolution: fixed resolution reason: Fix submitted Product-Group=junos

PR Number	Synopsis
1710975 SIRT=no	Bugatti: Tracking PR to separate out PMB BIOS binaries with AR LC resolution: fixed resolution reason: Fix submitted Product-Group=junos
1741162 SIRT=no	MX304 fpc live cores not copied to RE (vjunos) resolution: fixed resolution reason: Fix submitted Product-Group=junos

PR Number	Synopsis
1732691 SIRT=no	Bugatti:: BFT1_SFB not come online after USB image installation resolution: fixed resolution reason: Fix submitted Product-Group=junos

PR Number	Synopsis
1681860 SIRT=no	Bugatti: Capture system state at early bootup before EVO Launch resolution: fixed resolution reason: Fix submitted Product-Group=junos
1792145 SIRT=no	JDI-REGRESSION:MX304:Host 0 PCI Device not responding 0x1304:0xe6 resolution: fixed resolution reason: Fix submitted Product-Group=junosvae

PR Number	Synopsis
1738647 SIRT=no	Bugatti: RCB: RE to RE link issue_RE1 status didn't show-up from RE0 but RE1 displayed RE0 status resolution: fixed resolution reason: Fix submitted Product-Group=junos
1778848 SIRT=no	Bugatti:TI firmware version to be shown in "show system firmware" resolution: fixed

	resolution reason: Fix submitted Product-Group=junos

PR Number	Synopsis
1771522 SIRT=no	jnxFruOfflineReason in jnx-chassis.mib missing recent additions to jam_ipc_offline_reason.h resolution: fixed resolution reason: Fix submitted Product-Group=junos
1780833 SIRT=no	[JDI-RCT-DCF_EVPNVXLAN_MPLSL2Stitching_MX304]: Core-spmbpfe observed on MX304 gateway after loading base_config resolution: fixed resolution reason: Fixed in component Product-Group=junos

PR Number	Synopsis
1727052 SIRT=no	JDI-RCT:M/Mx: post ISSU in MXVC, vcp ifl went down and fpcs were restarted resolution: fixed resolution reason: Fix submitted Product-Group=junos
1766264 SIRT=no	Ksyncd core seen just after adding first VCP link while bringing up MXVC. resolution: fixed resolution reason: Fix submitted Product-Group=junos

PR Number	Synopsis
1701220 SIRT=no	[Amazon] jnxOperatingBufferExt shows 0 on ptx1 platform. resolution: fixed resolution reason: Fix submitted Product-Group=junos

PR Number	Synopsis
1712110 SIRT=no	irb rewrite-rule vlan-tag option is hidden in CLI and not allowed by other load method like load set terminal or xml or netconf resolution: fixed resolution reason: Fix submitted Product-Group=junos
1774312 SIRT=no	JUNOS_REG: mx240: While validating interface Ifd Queue Stats on egress forwarding-class best-effort observing statistics are not showing in-range resolution: fixed resolution reason: Fix submitted Product-Group=junos
1786911 SIRT=no	AUTO-CORE-PR : AUTO-CORE-PR:VIRTUAL_REG : COSD core found @ cosd_show_fabric_scheduler_map ms_parse_substring ms_parse_line_ex resolution: fixed resolution reason: Fix submitted Product-Group=junos
1787036 SIRT=no	[US FED] L3 Inject TWAMP Client probes are not classified correctly in Ukern Based linecards resolution: fixed resolution reason: Fix submitted Product-Group=junos
1789456 SIRT=no	[US FED] CBF Feature is broken when multiple forwarding classes are mapped to the same COS queue for host-injected L3 TWAMP probes resolution: fixed resolution reason: Fix submitted Product-Group=junos

PR Number	Synopsis

1770822 SIRT=no	DT_BNG: CoS adjustment fallback not working for static IFLSET on dynamic IFLSET resolution: fixed resolution reason: Fix submitted Product-Group=junos

PR Number	Synopsis
1676327 SIRT=no	CFM Core seen when egress IFL not set for CCC Local switching when configured with ae interface resolution: fixed resolution reason: Fix submitted Product-Group=junos
1739058 SIRT=yes	CFMD core at cfmd_show_ccc_mip_information when run "'show oam ethernet connectivity-fault-management mip" cmd resolution: fixed resolution reason: Fix submitted Product-Group=junos

1779066 SIRT=no	Bridge: CFM is not working on an interface with vlan-id-list configuration resolution: fixed resolution reason: Fix submitted Product-Group=junos

PR Number	Synopsis
1701508 SIRT=no	NULL_RETURNS:DEV_COMMON_BRANCH resolution: fixed resolution reason: Fix submitted Product-Group=junos
1748200 SIRT=no	Add a syslog for Non EUI64 compliant Link local IP address received as DHCP source IP resolution: fixed resolution reason: Fix submitted Product-Group=junos

PR Number	Synopsis
1657422 SIRT=no	TC 7.2-8. After restart l2ald, client gets re-authenticated on re-auth for L3 dot1x interface. resolution: fixed resolution reason: Fix submitted Product-Group=junos
1730561 SIRT=no	default mac filters are not installed when firewall restarted. resolution: fixed resolution reason: Fix submitted Product-Group=junos
1774687 SIRT=no	Mac is learnt on configured access vlan interface when we send a Suplicant-Mode-Single AV pair from radius during reauth resolution: fixed resolution reason: Fix submitted Product-Group=junos
1776006 SIRT=no	Port bounce attribute from radius server doesnt work when there are two users with same User name in dot1x resolution: fixed resolution reason: Fix submitted Product-Group=junos
1778901 SIRT=no	Dotx1 authentication issues with camera resolution: fixed resolution reason: Fix submitted Product-Group=junos

PR Number	Synopsis

1725158 SIRT=no	Received EVPN Type3 interconnect routes do not include route-label in show command response resolution: fixed resolution reason: Fix submitted Product-Group=junos
1747793 SIRT=no	DCF11 - ARP entry for remote Type2 symmetric host mac-ip is updated in DC-GW device resolution: fixed resolution reason: Fix submitted Product-Group=junos
1775495 SIRT=no	EX4400-48MP BUM traffic broken for dot1x auth vlans resolution: fixed resolution reason: Fix submitted Product-Group=junos
1781048 SIRT=no	PCT : RPD PC EVPN MCAST OISM IGMPv2 L3 VQFX: Multicast traffic forwarding to PEG is failing resolution: fixed resolution reason: Fix submitted Product-Group=junos
1790454 SIRT=no	Apstra DC Reference ERB Design: After clearing bgp neighborship dest mac is not programmed on the mac table though RPD has mac/IP received f MH peer resolution: fixed resolution reason: Fix submitted Product-Group=junos

PR Number	Synopsis
1736083 SIRT=yes	SSH is enabled by default even though there is no config allowing SSH access resolution: fixed resolution reason: Fix submitted Product-Group=junos
1738949 SIRT=no	SSH when using only ED25519 does not work after upgrade resolution: fixed resolution reason: Fix submitted Product-Group=junos
1755335 SIRT=	CVBC: SSH is enabled by default even though there is no config allowing SSH access resolution: fixed resolution reason: Document fixed Product-Group=junos

PR Number	Synopsis
1731662 SIRT=yes	Turn the Crank: OpenSSL 1.1.1u resolution: fixed resolution reason: Fix submitted Product-Group=junos
1756370 SIRT=yes	Turn the Crank: OpenSSL 1.0.2zi resolution: fixed resolution reason: Fix submitted Product-Group=junos

PR Number	Synopsis
1709843 SIRT=no	TEF: Family on Ifl utilized in hybrid evpn-vpls routing-instance is not programmed once moved from one routing-instance to the other and old VPL removed - in some cases, family vpls is programmed while family bridge is configured resolution: fixed resolution reason: Fix submitted Product-Group=junos
1717576 SIRT=no	EX4400: Allows to remove all the members from ae interface when minimum link is configured as 1 resolution: fixed resolution reason: Fix submitted

	Product-Group=junos
1778705 SIRT=no	SRX345:VDSL: DCD core at ../../../../../../src/bsd/lib/libc/mips/string/strlen.S:48 while pushing PPPoE over ADSL interface configurations from side resolution: fixed resolution reason: Fix submitted Product-Group=junos

PR Number	Synopsis
1678807 SIRT=no	NULL_RETURNS:DEV_COMMON_BRANCH resolution: fixed resolution reason: Fix submitted Product-Group=junos
1712666 SIRT=yes	vpls family filter with term "from traffic-type unknown-unicast" affects known-unicast traffic resolution: fixed resolution reason: Fix submitted Product-Group=junos

PR Number	Synopsis
1771497 SIRT=no	24.1DCB:vSRX3.0:SRX-RIAD : VSRX: Interfaces address not deleted for untrust security-zone, after the deleting interface dhcp-client configuratior resolution: fixed resolution reason: Fix submitted Product-Group=junos

PR Number	Synopsis
1710668 SIRT=yes	[ACX710] EVPN with native-vlan-id resolution: fixed resolution reason: Fix submitted Product-Group=junos
1766894 SIRT=no	IPV6 NA filter action should be changed from Redirect to Snoop resolution: fixed resolution reason: Fix submitted Product-Group=junos

PR Number	Synopsis
1758170 SIRT=no	[ACX5448]FPC status became empty after vmhost reboot to upgrade code from 20.4X50.2 to 21.4R3-S3.4 resolution: fixed resolution reason: Fix submitted Product-Group=junos

PR Number	Synopsis
1757549 SIRT=no	ACX710 - PFE is not coming up with device EEPROM from vendor ONSEMI resolution: fixed resolution reason: Fix submitted Product-Group=junos

PR Number	Synopsis
1737727 SIRT=yes	rpd memory crash due to the increase on MSPW SPE TLV resolution: fixed resolution reason: Fix submitted Product-Group=junos

PR Number	Synopsis

1801667 SIRT=no	[ACX7100-48L] MC-LAG active-active - MAC sync not working with GARP resolution: fixed resolution reason: Fix submitted Product-Group=junos

PR Number	Synopsis
1740602 SIRT=no	[evpn_vxlan] [evpn_instance] ACX7100-48L :: JDI-RCT:L2ald core observed "l2ald_enh_rnh_delete, l2ald_iff_del_ucst_nh ()" after loading ERB Mac profile configs resolution: fixed resolution reason: Fix submitted Product-Group=junos

PR Number	Synopsis
1756320 SIRT=no	SRX4600: show security advance-policy-based-routing statistics values are negative resolution: fixed resolution reason: Fix submitted Product-Group=junos

PR Number	Synopsis
1726701 SIRT=no	22.4R2:SRX5400:MNHA:Flow sessions and persistent-nat-table are empty after upgrade to 22.4R2.3 when nat source is configured resolution: fixed resolution reason: Fix submitted Product-Group=junos
1766880 SIRT=no	23.4R1:Appid:appid core dumped at ../../../../../../src/ui/include/ddl/dbs_offset.h:67 resolution: fixed resolution reason: Fix submitted Product-Group=junos
1788953 SIRT=no	SRX345/22.2R3-S2.8: Flowd core in jdpi_free_internal resolution: fixed resolution reason: Fix submitted Product-Group=junos

PR Number	Synopsis
1737875 SIRT=no	l2ald cores found during scriptrun resolution: fixed resolution reason: Fix submitted Product-Group=junos

PR Number	Synopsis
1763759 SIRT=no	FPC/PFE prompt not correctly display after installing JSU in 21.2R3-S4 code on MX2020 resolution: fixed resolution reason: Fix submitted Product-Group=junos

PR Number	Synopsis
1722482 SIRT=no	JUNOS_REG:MX-GNF: jdmd core is observed while performing jdm operations in dvaita inchassis. resolution: fixed resolution reason: Fix submitted Product-Group=junosvae
1790164 SIRT=no	JUNOS_REG:Dvaita: Unable to delete the JDM in dvaita inchassis in 24.1 TH builds resolution: fixed resolution reason: Fix submitted

	Product-Group=junos

PR Number	Synopsis
1732213 SIRT=no	Rio-Odin-EOAMoEVPN: Incorrect SLM stats reflected after cfm restart resolution: fixed resolution reason: Fix submitted Product-Group=junos
1745076 SIRT=no	DT_BNG: cfmd core at Address not mapped to object. #0 get_md_status (md=0x2794540, vlan=0) at ../../../../../../src/junos/usr.sbin/cfmd/cfmd_mthd.c:3347 3347 if ((md_iter -> cfm_level == md -> cfm_level) && (!md -> cfm_default_md)) resolution: fixed resolution reason: Fix submitted Product-Group=junos

PR Number	Synopsis
1446571 SIRT=no	administrative PR for RPD pointer update resolution: fixed resolution reason: Fix submitted Product-Group=junos

PR Number	Synopsis
1271624 SIRT=no	Administrative PR: Update libjnh-proxy pointer for junos libjnh image resolution: fixed resolution reason: Fix submitted Product-Group=junos

PR Number	Synopsis
1760938 SIRT=no	Re-integrate "traceroute monitor" CLI command for EVO resolution: fixed resolution reason: Fix submitted Product-Group=junos
1762262 SIRT=	CVBC: Re-integrate "traceroute monitor" CLI command for EVO resolution: fixed resolution reason: Document fixed Product-Group=junos

PR Number	Synopsis
1769720 SIRT=no	CCL anCX : fibtd cored at #1 ipc_pipe_read_clean (pipe=0x7b20746e6576650a) at ../../../../../../src/dsa/lib/jipc/ipc_pipe.c:531 resolution: fixed resolution reason: Fix submitted Product-Group=junos

PR Number	Synopsis
1771564 SIRT=no	Deplayer // Disable on ULC. resolution: fixed resolution reason: Fix submitted Product-Group=junos

PR Number	Synopsis
1756662 SIRT=no	Error in show version detail output resolution: fixed resolution reason: Fixed in component Product-Group=junos